Daily Open Source Infrastructure Report
3 April 2012

Top Stories

- The Department of Energy identified serious cybersecurity gaps at the Bonneville Power Administration, which supplies wholesale electric power to regional utilities in the Pacific Northwest. – *Infosecurity* (See item **2**)
- A data breach at the Global Payments payments processing firm potentially compromised up to 1.5 million credit and debit card numbers from all of major card brands. – *CNNMoney* (See item **7**)
- The Department of Agriculture confirmed that citrus greening, a plant disease that has killed millions of citrus trees and cost growers billions of dollars across Florida and Brazil, was detected in California. – *Associated Press* (See item **18**)
- A bomb squad discovered wired explosives, chemicals, and gunpowder in the apartment of a dead man in Mont Belvieu, Texas, prompting an evacuation. – *KRIV 26 Houston* (See item **51**)

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 1, Agence France-Presse* – (International) **North Sea gas rig blast averted.** A flare that threatened to cause an explosion at a North Sea platform has gone out, its operator said March 31, but a plume of highly flammable gas was still leaking from the stricken rig. There had been fears that the cloud of gas, which continues to leak from the platform at a rate of an estimated 200,000 cubic metrers per day, could come into contact with the flame and ignite, causing a massive explosion. "There is still a gas escape, and clearly escaping gas is always at risk of ignition and explosion," Total's U.K. communications manager said. A spokesman at the firm's Paris headquarters stated Total was losing revenues of $1.5 million every day as a result of the shutdown of production at Elgin. The company is preparing to sink two relief wells to stop the gas leak.
   Source: http://www.calgaryherald.com/North+blast+averted/6393190/story.html

2. *March 30, Infosecurity* – (National) **Serious cybersecurity lapses found at Pacific Northwest electricity supplier.** The Department of Energy (DOE) identified serious cybersecurity gaps at the Bonneville Power Administration, which supplies wholesale electric power to regional utilities in the Pacific Northwest, Infosecurity reported March 30. An audit by DOE's Office of the Inspector General (OIG) found Bonneville did not implemented controls designed to address known IT system vulnerabilities. "Specifically, technical vulnerability scanning conducted on nine applications used to support business functions such as financial management, human resources, and security management identified a significant number of high-risk weaknesses in the areas of access controls, patch management, and validation of user input," according to the audit. In addition, OIG's testing of five operational security control systems identified issues with configuration management, access controls, and contingency and security planning. A number of IT system development efforts suffered from cost, scope, and schedule overruns due to weaknesses in project planning and management.
   Source: http://www.infosecurity-magazine.com/view/24869/serious-cybersecurity-lapses-found-at-pacific-northwest-electricity-supplier/

3. *March 30, Nanuet Patch* – (New York) **Stony Point man charged in $50K copper wire theft from O&R in West Nyack.** A Stony Point, New York man was arrested in connection with the theft of a $50,000 supply of copper wire reported stolen from an Orange and Rockland Utilities (O&R) substation in West Nyack in February, Clarkstown police said March 30. The man was charged with third-degree grand larceny by members of the Clarkstown Detective Bureau who investigated the theft reported February 22 at the substation at 195 Route 59. The wire, about 2,592 linear feet of it, was discovered missing when an O&R worker went to the substation. Police said the man, a home-improvement contractor, is believed to have had help in hauling

away the wire from West Nyack and then bringing it in several loads to a scrap metal dealer in Westchester County. Police said several other people are being sought in connection with the theft.
Source: http://nanuet.patch.com/articles/stony-point-man-charged-in-50k-copper-wire-theft-from-o-r-in-west-nyack

For another story, see item **52**

[Return to top]

Chemical Industry Sector

4. *March 30, KXAS 5 Dallas-Fort Worth* – (Texas) **OSHA cites Magnablend following massive fire.** Magnablend Inc. is facing $45,000 in proposed fines imposed by Department of Labor's Occupational Safety and Health Administration (OSHA) for seven safety and health violations following a massive fire at their blending plant in Waxahachie, Texas, in 2011, KXAS 5 Dallas-Fort Worth reported March 30. OSHA's Fort Worth office "found that employees were exposed to fire hazards due to inadequate ventilation, which can create an accumulation of flammable vapors that lead to a fire or explosion," the U.S. Department of Labor said March 30 in a news release. "The violations are failing to conduct a hazard assessment, install a sufficient ventilation system, train workers in specific hazardous chemical protection procedures, evaluate respiratory inhalation hazards, ensure that the fire sprinkler system was adequate, use electrical equipment in accordance with its labeling, document the classification of hazardous locations for electrical purposes and ensure that electrical equipment was considered safe for the location where it was used."
Source: http://www.nbcdfw.com/news/local/OSHA-Cites-Magnablend-Following-Massive-Fire-145207255.html

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *April 2, Professional Reactor Operator Society* – (International) **Cracks detected again in Swedish reactor control rods.** Small cracks were again detected in control rods used to control the fission process at two nuclear reactors at the Forsmark nuclear power plant in Sweden, media reports said March 28. Cracks were detected in 2011 at one reactor at Forsmark and one reactor at the Oskarshamn plant, in south- eastern Sweden. Several control rods were replaced at the end of 2011, but some of the new rods appeared to have faults. Oskarshamn plant's chief executive told Swedish radio news that the new rods may have been damaged at production, but a probe was underway.
Source: http://www.nucpros.com/content/cracks-detected-again-swedish-reactor-control-rods

6. *March 30, Bloomberg* – (South Carolina) **Scana receives NRC approval to build South Carolina reactors.** Scana Corp. won U.S. approval to build two new nuclear

reactors at the Virgil. C Summer plant in Fairfield County, South Carolina, the second construction permit issued by regulators in more than 30 years. The Nuclear Regulatory Commission, March 30 voted 4-1 to approve the company's plan to construct and operate two Westinghouse AP1000 units. The second unit is planned to be operational by 2018, according to the company.
Source: http://www.bloomberg.com/news/2012-03-30/scana-receives-nrc-approval-to-build-south-carolina-reactors-1-.html

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

7. *April 2, CNNMoney* – (International) **1.5 million card numbers at risk from hack.** A data breach at a payments processing firm potentially compromised up to 1.5 million credit and debit card numbers from all of major card brands. Global Payments, a company that processes card transactions, confirmed March 30 that "card data may have been accessed." It said it discovered the intrusion in early March and "promptly" notified others in the industry. Global Payments released a statement April 1 with more details. The company said that while more than 1 million card numbers were potentially compromised, cardholder names, addresses, and Social Security numbers were not affected. Global Payments did not say which card companies were affected, but Visa released a statement March 30 saying it was all of the major companies. MasterCard said it alerted payment card issuers "regarding certain MasterCard accounts that are potentially at risk." Discover and American Express said they are monitoring the situation. Global Payments held a conference call April 2 to provide more details on the debacle. Executives stressed that an investigation is ongoing. Until the investigation is complete, they are waiting to release specifics on how the hack occurred. A U.S. Secret Service spokesman said March 31 the agency also is investigating the incident. Global Payments said the breach was limited to only "a handful of servers," and appears to be confined to accounts in North America. Global Payments processed $167 billion worth of transactions in its last fiscal year.
Source: http://money.cnn.com/2012/04/02/technology/global-payments-breach/

8. *April 2, Associated Press* – (Nevada; National) **FTC targets alleged payday scam, race car driver.** A payday lending operation that offers quick cash over the Internet to

desperate people, and the race-car driver allegedly running it, are under federal scrutiny after more than 7,000 complaints to authorities, the Associated Press reported April 2. The Federal Trade Commission (FTC) filed a complaint in U.S. district court in Nevada against the driver, his brother, and several Internet-based lending companies, including AMG Services, Inc. The FTC charges that the driver and others controlled lending companies that piled on undisclosed and inflated fees — in some cases more than triple the amount borrowed — and then collected on the loans illegally by threatening borrowers with arrests and lawsuits. In one example, a consumer was told a $500 loan would cost him $650 to repay. Instead, the FTC says, the defendants attempted to charge him $1,925 to pay off the loan. The agency said he was threatened with arrest if he did not pay that amount. Over the last 5 years, more than 7,500 complaints about the operation were filed with law enforcement authorities. The driver and his brother are accused of transferring more than $40 million collected from payday loans to consumers to another company, Level 5 Motor Sports. The FTC said the money was transferred as "sponsorship" fees for the drivers racing career.
Source: http://www.miamiherald.com/2012/04/02/2727611/ftc-targets-alleged-payday-scam.html

9. *April 2, Associated Press* – (International) **Temporary outage of Visa card network Sunday.** A technical problem affecting the Visa network barred some people around the United States from using their credit and debit cards for about 45 minutes April 1, the company said. The outage was caused by a recent update Visa made to its system, a Visa Inc. spokeswoman said. She said Visa had trouble processing some transactions as a result, but the system is operating normally now. The spokeswoman said the problem was unrelated to the security breach potentially affecting Visa and MasterCard customers reported March 30 by credit card processor Global Payments Inc. The outage occurred from around 2:40 p.m. to 3:20 p.m., a person from a major bank said. Visa notified the banks that are members of its network of the problem. Consumers and merchants reported having Visa cards rejected April 1.
Source: http://www.wishtv.com/dpps/money/business_news/temporary-outage-of-visa-card-network-sunday-nt12-jgr_4124112

10. *April 1, Fort Worth Star-Telegram* – (Texas; International) **Computer hacker tries to steal $1.8 million from Arlington's bank account.** A computer hacker tried to steal $1.8 million from the city of Arlington, Texas' bank account in late February, but officials would not release details, citing an ongoing investigation. City treasury staff, using internal audit controls, detected the fraudulent transfers and recovered the money, an Arlington spokeswoman told the Fort Worth Star-Telegram March 31. It was not revealed how and when the hacker accessed the account information, how much was in the account, or what the city did to improve security. Arlington Police initially handled the investigation, but a source said the FBI is taking over. After the breach, the spokeswoman said the city is reviewing systems and control measures and is working closely with security consultants, banking regulators, and investigators.
Source: http://www.star-telegram.com/2012/04/01/3850876/computer-hacker-tries-to-steal.html#storylink=cpy

11. *March 30, Douglasville Patch* – (Georgia) **Douglasville business involved in identity theft scheme.** A jury in Atlanta's federal district court returned a guilty verdict March 29 against two defendants on charges of stealing the identities of more than 85 individuals in the Atlanta area. According to a U.S. attorney, between May 2006 and March 2010, the pair stole mail, credit cards, and other personal information from individuals in the Atlanta area, and then opened a variety of financial accounts under the victims' names. As part of the scheme, one of the defendants obtained a job as a mail carrier in the Hiram Post Office under an identity she stole from another person from Nigeria before she entered the United States in 2004. She obtained a social security card and a U.S. passport and, in March 2009, was naturalized as a U.S. citizen — all under the assumed name. Using the information stolen from the mail route customers, the pair applied for credit cards and bank loans in their victims' names. They deposited the fraudulent loan proceeds into bank accounts opened under yet other victims' names and then wrote checks from those accounts to their two fraudulent businesses, GMO Auto Services in Douglasville and Gabmike Limousine Service in Smyrna. They also used the fraudulent credit cards at their businesses. In March 2010, law enforcement officers stopped the defendants driving a Lincoln Navigator and found dozens of American Express, Walmart, and Target gift cards that were purchased with stolen credit cards issued to individuals residing on the woman's mail route. The jury returned guilty verdicts on all 44 counts it considered, including conspiracy, access device or credit card fraud, aggravated identity theft, bank fraud, mail theft, immigration fraud, social security fraud, and passport fraud.
    Source: http://douglasville.patch.com/articles/douglasville-business-involved-in-identity-theft-scheme

[Return to top]

Transportation Sector

12. *April 2, Reuters* – (Kansas) **Five die, 13 injured in Kansas truck crash.** Five people died and 13 were injured April 1 when the large truck equipped as a motor home they were riding in left a rural Kansas freeway and careened into a creek, the Kansas Highway Patrol said. The rig involved in the crash was towing a trailer north on Interstate 35 in Osage County. The vehicle went off the highway, hit a metal guard rail, and then a concrete bridge rail before tumbling down into a creek, the patrol said. The truck landed on its wheels and the trailer ended up in front of the truck. Thirteen people were taken to area hospitals, the patrol said. The cause of the crash remained under investigation.
    Source: http://news.yahoo.com/five-die-13-injured-kansas-truck-crash-043538412.html

13. *April 2, WRIC 8 Richmond* – (Virginia) **Eleven hurt In I-64 school bus crash.** A school bus was involved in a crash on I-64 eastbound in Richmond, Virginia, carrying students from Manchester Middle School to the Math and Science Innovation Center, WRIC 8 Richmond reported April 2. Eleven people were transported to the hospital, including several children. The crash also involved a GRTC van, a tractor trailer, and a passenger car. Hospital officials said all of the victims had minor injuries. The crash was located in the eastbound lanes of Interstate 64 just east of the Mechanicsville

Turnpike exit.
Source: http://www.wric.com/story/17310077/crash-involving-bus-on-i-64

14. *April 1, WFAA 8 Dallas* – (Texas) **'Robotic device' triggers evacuation at Dallas Love Field.** Dallas Love Field in Texas was shut down April 1 after a Southwest Airlines jet bound for Amarillo was found with a suspicious device on board. The Transportation Security Administration said passengers were evacuated from Gates 3 to 15 "out of an abundance of caution." A City of Dallas spokesman said a "robotic device" was found near the cockpit of Southwest Airlines Flight 157 after it arrived from Kansas City. Air marshals and Love Field security officers detained 11 passengers — including students and their professor — who were linked to the gizmo. "It was determined that the device was not dangerous and was a student's science project," the spokesman said in a written statement. "The student told authorities the robot was accidentally left on the plane."
Source: http://www.wfaa.com/news/local/Love-Field-evacuation-was-false-alarm-145697115.html

15. *March 31, Newsday* – (National) **TSA urged to review plastic airline handcuffs.** The chair of the House Homeland Security Committee said March 30 that "use of plastic restraints will be one of the many things that will be fully investigated," and asked the Transportation Security Administration (TSA) to review security procedures after plastic handcuffs apparently failed to subdue a disturbed pilot on a flight from New York City to Las Vegas March 27, Newsday reported March 31. There is no federal requirement that aircraft have restraints such as plastic handcuffs on board, although airlines and independent aviation security experts said it is industry practice to carry such devices and that flight crews are trained in how to use them. An airline consultant with more than 40 years in the industry, said the failure of the handcuffs on JetBlue Flight 191 appears to be a manufacturing problem. The restraints are routinely used successfully and the government does not need to change its hands-off approach. "The times that I have been involved in their use, they have worked very well," the airline consultant stated. A JetBlue spokeswoman said crews are trained to use "strengthened plastic flex-cuffs." The devices, the spokeswoman said, are approved by government regulators.
Source: http://www.heraldnet.com/article/20120331/NEWS02/703319926

16. *March 30, Associated Press* – (Illinois) **NATO summit could shut down Chicago rails.** Security plans for the NATO summit in Chicago could include a shutdown of vital passenger rail and freight lines running beneath the venue, disrupting the routines of thousands of commuters living in the southern suburbs and northern Indiana at the start of the week of April 2, the Associated Press reported March 30. Two major commuter lines, a freight route and Amtrak service to points as far away as New Orleans all run underneath the sprawling McCormick Place convention center near Lake Michigan. The rail services involved said March 30 they have been talking with the Secret Service about security arrangements that could include closures. The final day of the May 20-21 summit falls on a Monday, when there would be about 18,000 commuters alone on the Metra Electric, which has 172 trains a day barreling under McCormick Place. There is also an intra-city baseball matchup that weekend that could

push up passenger numbers.
Source: http://www.nola.com/newsflash/index.ssf/story/nato-summit-security-could-shut-down-chicago/9a765be8422a41989f34c53c5754e9c6

For another story, see item **52**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

17. *April 1, Oklahoma City Oklahoman* – (Oklahoma) **Ammonia fumes at Oklahoma food plant sicken four.** One person was hospitalized and three more treated at the scene April 1 when ammonia fumes caused them to fall ill at a Moore, Oklahoma food plant, authorities said. Firefighters were called to Vaughan Foods, Inc. to check for the fumes which sickened the employees, the Moore deputy fire chief said. The building was evacuated, and the cause was determined to be an outdoor container with an ammonia product used for cleaning and refrigeration. The fumes were blown into the building by winds. Crews were expected to be at the scene for several hours.
Source: http://newsok.com/ammonia-fumes-at-oklahoma-food-plant-sicken-four/article/3662884#ixzz1qtHuGGNa

18. *April 1, Associated Press* – (National) **Deadly citrus disease turns up in California.** A citrus disease that has killed millions of citrus trees and cost growers billions of dollars across Florida and Brazil has been detected in California, despite the industry's best efforts to keep it at bay, the Associated Press reported April 1. After a week of testing the U.S. Department of Agriculture confirmed citrus greening was detected in a lemon-grapefruit hybrid tree in a residential neighborhood of Los Angeles County. The disease stands to threaten not only California's nearly $2 billion citrus industry but backyard trees scattered throughout the state. "Huanlongbing is called the world's worst disease of citrus," said an official with the California Department of Food and Agriculture. The bacterial disease is carried by the Asian citrus psyllid and attacks a tree's vascular system, producing bitter fruit and eventually killing the tree. Sap-sucking pysllids that feed on an infected tree become carriers of the disease. The disease is present in Mexico and across the southern U.S., but nowhere is the problem more severe than in Florida, where the disease first appeared in 2005. The University of Florida estimates it has cost 6,600 jobs, $1.3 billion in lost revenue to growers, and $3.6 billion in lost economic activity. The pest and the disease also are present in Texas, Louisiana, Georgia, and South Carolina. The states of Arizona, Mississippi, and Alabama have detected the pest but not the disease.
Source:
http://nhregister.com/articles/2012/04/01/news/doc4f7908eb4ddbc220182535.txt

19. *March 31, Food Safety News* – (New York) **NYC investigating possible tofu-related botulism cases.** The New York City Department of Health and Mental Hygiene is investigating one confirmed and one suspect case of botulism and issued a warning about unrefrigerated fresh bulk tofu. The tofu is the possible but unconfirmed source of the illnesses, Food Safety News reported March 31. Both patients are Queens residents who recently purchased unrefrigerated fresh bulk tofu from the same store in Flushing, the health department said. The tofu was not made at the store, and its source was still under investigation.
Source: http://www.foodsafetynews.com/2012/03/nyc-health-officials-investigating-botulism-cases/

20. *March 31, Food Safety News* – (National) **Pita breads, sandwich rolls recalled.** Wegmans is recalling specific date codes of its Pita Breads and Thin Sandwich Rolls because they may contain bits of metal or plasticized fabric from a damaged conveyor belt, Food Safety News reported March 31. The recalled pita breads and sandwich rolls would have been purchased March 28 only.
Source: http://www.foodsafetynews.com/2012/03/pita-breads-sandwich-rolls-recalled/

21. *March 31, Food Safety News* – (National) **Allergen alert: Cream puffs with sodium caseinate.** Creme Curls Bakery of Hudsonville, Michigan, recalled 19.4 ounce cartons of Simply Enjoy Vanilla cream puffs distributed by Foodhold U.S.A., and 13.2 ounce cartons of Vanilla Cream Puffs distributed by Creme Curls Bakery, because the product contains sodium caseinate. The sodium caseinate is listed on the label, but the label does not identify the source of the sodium caseinate as milk, Food Safety News reported March 31. The recall was initiated following a report of an allergic reaction after a person with a milk allergy ate the cream puffs. The recalled vanilla cream puffs were distributed nationwide through retail grocery stores.
Source: http://www.foodsafetynews.com/2012/03/allergen-alert-cream-puffs-with-unlabeled-milk-derivative/

22. *March 31, Food Safety News* – (National) **Chicken apple sausage may contain plastic pieces.** Eddy Packing Co. of Yoakum, Texas, recalled approximately 26,136 pounds of chicken apple sausages that may contain foreign materials, the U.S. Department of Agriculture's Food Safety and Inspection Service announced March 31. The problem was discovered as a result of consumer complaints about finding pieces of plastic in the product. The recall includes: 1-pound vacuum-sealed, 3 to a pack of "ARTISAN FRESH, ALL NATURAL chicken & apple sausage" and 36-pound cases of "ARTISAN FRESH, ALL NATURAL CHICKEN APPLE SAUSAGE." The sausages were produced February 9 and were distributed nationally through a warehouse chain February 14.
Source: http://www.foodsafetynews.com/2012/03/chicken-apple-sausage-may-contain-foreign-materials/

23. *March 31, Food Safety News* – (National) **Salmonella test prompts South Florida Produce to recall jalapeno peppers.** South Florida Produce recalled certain jalapeno peppers because they may be contaminated with Salmonella, Food Safety News reported March 31. The potential for contamination with the pathogen was noted during

a routine test by a retail store, which revealed the possible presence of Salmonella in packs of 2, 10, and 40 count packages, according to the U.S. Food and Drug Administration news release. This was the third recall announcement the week of March 26 related to the same suspect jalapeno peppers. The peppers recalled by South Florida Produce went to distributors in Oxford, North Carolina; Lake Worth, Florida; Washington, D.C.; Pompano Beach, Florida; Fair Lawn, New Jersey; and Toronto, Ontario, Canada via customer truck March 5 through 7. Castellini Company recalled jalapenos distributed from its Wilder, Kentucky facility because they had the potential to be contaminated with Salmonella. Club Chef recalled certain salsas because they had the potential to be contaminated with Salmonella from jalapenos, an ingredient. A random test by the Ohio Department of Agriculture in a store in Ohio revealed the presence of Salmonella in a case of jalapeno peppers.
Source: http://www.foodsafetynews.com/2012/03/more-jalapeno-peppers-recalled/

24. *March 31, Associated Press* – (Indiana) **Health officials: Illness traced to NE Ind. eatery.** Northeastern Indiana health officials said a suspected food-poisoning case that sickened at least 20 people was traced to Fort Wayne restaurant. The Fort Wayne-Allen County Department of Health said March 30 it was investigating the outbreak after receiving multiple reports from patrons who ate at Cebolla's Mexican Grill March 25. A department spokesman said test results were pending, but the symptoms are consistent with norovirus. He said early indications point to an employee who might have reported to work despite feeling ill. Health officials said the restaurant is fully cooperating with investigators.
Source:
http://www.indystar.com/usatoday/article/38935393?odyssey=mod|newswell|text|News|p

25. *March 31, Middletown Times Herald-Record* – (New York) **Ex-pharmacist from Town of Ulster held in Albany Medical Center mercury scare.** A retired pharmacist from Ulster, New York, was arrested March 30 in connection with planting poisonous mercury in an Albany Medical Center cafeteria. He was arrested after a joint investigation by the FBI, the Town of Ulster Police Department, Albany Medical Center, the state police, and the state Health Department. According to an Albany police officer, a small metal ball of liquid was found by a hospital employee in her order of chicken fingers March 2. A test determined the substance to be mercury, and an investigation turned up more mercury in the Albany Medical Center cafeteria. March 27, the hospital put out a $25,000 reward for information leading to the arrest and conviction of the person responsible. Detectives started investigating the suspect after receiving a phone tip from a person who recognized him from a surveillance video photo released by Albany police. The suspect is being charged with first-degree tampering with a consumer product, a felony. He was arraigned in Albany and sent to jail without bail.
Source:
http://www.recordonline.com/apps/pbcs.dll/article?AID=/20120331/NEWS/203310332

26. *March 30, Vallejo Times-Herald* – (California) **Nearly 100 sickened by carbon dioxide leak at Vallejo food processing plant; company owner calls incident 'false**

alarm'. A carbon dioxide leak at a food processing plant in Vallejo, California, sent 95 employees to the hospital March 30 for treatment of nausea, weakness, and breathing problems. Employees were evacuated from the Ghiringhelli Specialty Foods after one employee complained of weakness. Dozens of other employees soon complained of feeling ill, and firefighters set up an immediate triage center in the parking lot to treat employees who were vomiting and fainting. Firefighters pinpointed high carbon dioxide levels as the cause, but the plant's owner called the incident a "false alarm" and attributed some of the employees' symptoms to "anxiety." Employees told firefighters they started feeling ill after they turned on a freeze tunnel machine, which is connected to a large tank of carbon dioxide. The machine made an unusual noise, and a manager ordered it switched off. However, more people began to feel ill, firefighters said. Most of the ill employees were taken to local hospitals for treatment. Those not showing symptoms were taken by a Vallejo city bus to hospitals to be checked out. Using 20 ambulances, medical personnel transported 95 of the plant's 96 employees to hospitals, firefighters said. At least one patient was admitted and was in serious condition, a hospital official said. A road was closed to traffic for about 2 and a half hours during the evacuation.
Source: http://www.contracostatimes.com/top-stories/ci_20291800/vallejo-crews-respond-hazmat-scene

[Return to top]

Water Sector

27. *April 1, KRQE 13 Albuquerque* – (New Mexico) **Water main break closes high school.** A water main break March 31 in north east Albuquerque, New Mexico, shut down the Digital Media Arts Collaborative Charter School for one week. Water shot up from deep underground, pushing through the asphalt, and flinging dozens of rocks right at the school's windows. It took crews nearly three hours to get the 80 foot geyser under control. Damages range from deep puddles to soaked ceilings and damaged computers. Crews will assess structural damages, but until then students and staff are not allowed inside the building. Water was shut off to about 20 customers in the area through midnight. The water company says the pipe likely burst because it was so old.
Source: http://www.krqe.com/dpp/news/education/water-main-break-closes-high-school

28. *April 1, Buffalo News* – (New York) **Trace levels of toxins found in canal near former steel plant site.** Trace levels of radioactive uranium attributed to the former Guterl Steel plant in Lockport, New York, were found in water seeping through the walls of the Erie Canal, the U.S. Army Corps of Engineers said the week of March 26. The December 2011 sampling was the first time seeping ground water at the Ohio Street plant was tested, according to a program specialist for the Guterl site. However, testing of canal surface water in January 2012 showed no uranium, the Corps reported in a newsletter posted on its Web site. Seventeen ground water monitoring wells and the seepage from the nearby canal walls showed radioactive materials moving from the plant site. The testing was part of the run-up to a formal feasibility study on a possible cleanup plan for the polluted 18 acres, which includes a 9-acre landfill and the land

covered by the contaminated buildings, also known as the "excised property." The feasibility study should be completed by the end of 2012. The Corps' newsletter said the uranium seepage should not harm recreational use of the canal, and it said that uranium does not accumulate in fish.
Source: http://www.buffalonews.com/city/communities/lockport/article790628.ece

29. *April 1, Johnson County Daily Journal* – (Indiana) **Service restored after water main break.** Thousands of Indiana American Water customers in Franklin, Indiana, lost service and had to boil their water after pipes had to be repaired due to accidental water main damage, March 30. Repairs to a water main caused a pipe to shake, which resulted in about 10 additional water pipe breaks, an Indiana American spokesman said. A water tower was drained after the first water main break, and some parking lots filled with water. About 3,000 customers west of U.S. 31 were without water until the afternoon from the initial damage. About 50 customers lost water service due to the additional breaks. As of April 1, all water service was restored. The boil order ended March 31. Additional boil orders were issued for five customers affected by the subsequent breaks.
Source:
http://www.dailyjournal.net/view/local_story/Service_restored_after_water_m_1333326401/

30. *March 31, Middletown Record* – (New York) **Port wastewater plant gets $12.5M upgrade.** The New York City Department of Environmental Protection (DEP) finished a $12.5 million project to upgrade a wastewater treatment plant in Port Jervis, the Middletown Record reported March 31. The modernization of the 60-year old plant is aimed at protecting the water quality of the Neversink River and the Delaware River immediately downstream of the plant, according to the DEP. The plant has a permitted capacity of 2.5 million gallons a day, cut down from 5 million in late 2010 by the DEP. The DEP said they are still looking into whether to cut capacity even further.
Source:
http://www.recordonline.com/apps/pbcs.dll/article?AID=/20120331/NEWS/203310335/-1/SITEMAP

[Return to top]

Public Health and Healthcare Sector

31. *April 1, NewsCore* – (Florida) **Poison from suicide attempt shuts down Florida emergency room, sickens paramedics.** The emergency room at a Margate, Florida hospital was temporarily shut down for roughly 7 hours April 1 after a man who had attempted suicide vomited up poison, sickening three paramedics. The South Florida Sun-Sentinel reported that emergency rescue workers responded to a home of a man who tried to kill himself by drinking pesticide. As the paramedics transported the man to Northwest Medical Center he vomited, causing the rescuers "to become dizzy, nauseous" and suffer headaches. The man was brought into a containment area and the emergency room was closed as a precaution. The vehicle that transported the man to the hospital was put into quarantine. A hazardous materials team from the Broward

Sheriff's Office was called to the scene, and the three paramedics were treated for contamination sickness.
Source: http://www.foxnews.com/us/2012/04/01/poison-from-suicide-attempt-shuts-down-florida-emergency-room-sickens/

32. *March 30, Federal Bureau of Investigation* – (Florida) **Miami woman pleads guilty to participating in $200M Medicare fraud scheme.** A Miami-area resident pleaded guilty March 30 for his role in structuring monetary transactions to provide cash for the furtherance of a fraud scheme that resulted in the submission of more than $200 million in fraudulent claims to Medicare, according to an announcement by the Department of Justice, the FBI, and the Department of Health and Human Services. He admitted that he structured currency transactions to avoid reporting requirements so he could provide $2.4 million in cash to the owners and operators of American Therapeutic Corporation (ATC); its management company, Medlink Professional Management Group Inc.; and the American Sleep Institute (ASI). ATC operated purported partial hospitalization programs (PHPs) in seven different locations throughout south Florida and Orlando. ASI purported to provide diagnostic sleep disorder testing. According to court filings, ATC's owners and operators paid kickbacks to owners and operators of assisted living facilities and halfway houses and to patient brokers in exchange for delivering ineligible patients. According to court filings, to obtain the cash used to pay the kickbacks, the co-conspirators laundered millions of dollars of payments from Medicare and structured their transactions to avoid detection by bank officials and the authorities.
Source: http://www.loansafe.org/miami-woman-pleads-guilty-to-participating-in-200m-medicare-fraud-scheme

[Return to top]

Government Facilities Sector

33. *April 2, Associated Press* – (Indiana) **School resumes for all from tornado-hit Ind. town.** Some 500 students headed back to class for the first time since a tornado devastated their southern Indiana school in March. Henryville Junior-Senior High School students were to arrive April 2 at the Mid America Science Park in Scottsburg, Indiana, where conference rooms and store rooms were converted into classrooms, computer labs, and a cafeteria. The West Clark schools assistant superintendent said the district was trying to help students get back in the academic groove following the March 2 storm. Elementary students returned to school March 21 at a rented church building in New Albany.
Source: http://www.cbsnews.com/8301-501363_162-57407940/school-resumes-for-all-from-tornado-hit-ind-town/

34. *April 2, WGAL 8 Lancaster* – (Pennsylvania) **Federal agent investigates fire at Lebanon School.** A federal agent was investigating a fire at Willow Street Academy in Lebanon, Pennsylvania, April 2. The city's fire chief called the fire suspicious and an agent from the Bureau of Alcohol, Tobacco, Firearms, and Explosives was at the scene investigating. Classrooms and the cafeteria were damaged in the building that is owned

by Calvary Chapel Lebanon. Ninth graders in the Lebanon City School District were using the school while their regular building is renovated. Classes were cancelled April 2.
Source: http://www.wgal.com/r/30815961/detail.html

35. *March 31, Associated Press* – (California) **Candidates seek restitution after fraud plea.** A California campaign treasurer pleaded guilty March 30 to defrauding at least $7 million from a high-profile roster of politicians in the largest embezzlement case of its kind. But the resolution of the criminal case is expected to do little to help victims recover money they lost in the scheme that the U.S. attorney said highlights the shortage of regulations governing campaign finance managers. The defendant entered her pleas to five counts of mail fraud in a U.S. district court in Sacramento. Prosecutors said the woman ran a complex shell game from her Burbank office in which she shifted millions of dollars between bank accounts for politicians, community groups, personal accounts, and those of her business, Durkee & Associates. The U.S. attorney believes the actual fraud was closer to $10 million. The woman's scheme relied on the trust of her victims, who included a U.S. Senator, who has said she lost $4.5 million, along with members of Congress and state lawmakers. The deception has left numerous candidates with little or no money in their campaign accounts, which have been frozen since the woman's arrest. Prosecutors said the woman controlled some 700 bank accounts.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5g5gNstz79MgwMgGCKfV1TjsYNAFw?docId=53a562019872403d9d363acc51332342

For more stories, see items **10**, **13**, and **46**

[Return to top]

Emergency Services Sector

36. *April 2, Philadelphia Inquirer* – (New Jersey) **Rogue N.J. officers cost city $340K in damages.** Eleven people whose convictions were overturned because of potentially tainted evidence gathered by corrupt Camden, New Jersey city police were awarded $340,000 in damages, and 64 related suits are under review in state Superior Court, the Philadelphia Inquirer reported April 2. Four former police officers were convicted of planting evidence, stealing cash and drugs, conducting illegal searches, and fabricating reports that led to a series of arrests and convictions between 2007 and 2009. Each faces about 10 years in jail. More than 200 of their cases were dismissed or vacated after the Camden County Prosecutor's Office learned of the corruption allegations. Civil suits in New Jersey Superior Court were filed by 75 people, as well as in federal court from almost as many individuals. Most of the plaintiffs had drug convictions that predated the arrests and imprisonments for which they seek compensation.
Source:
http://www.philly.com/philly/news/20120402_Camden_rogue_police_cost_New_Jersey__340_000_in_damages.html

37. *March 30, WRTV 6 Indianapolis* – (Indiana) **Bloomington man called hero in deputy struggle.** The Monroe County Sheriff's Department is crediting a Bloomington, Indiana man for saving a deputy's life, WRTV 6 Indianapolis reported March 30. A sheriff's deputy was with a suspect en route to the Monroe County Jail when detectives said the suspect somehow got his handcuffs in front of his body while in a seat belt in the back of the deputy's SUV and brought his arms around the deputy's neck, and then reached for her gun. The gun went off, narrowly missing the deputy's leg. A man nearby said he heard the deputy scream and rushed to help. "I opened the door and jumped on (the suspect's) back. I put him in a headlock and pried him off (the deputy)," he said. The man tore a ligament in his hand during the violent struggle and said he heard the suspect tell the deputy she "Wouldn't get out of the car alive." Monroe County Sheriff's Department officials also commended the man and said they expect he will be formally recognized by the sheriff.
Source: http://www.theindychannel.com/news/30805597/detail.html

38. *March 30, San Jose Mercury News* – (California) **Concord man pilfered firefighting equipment over the past year, officials say.** A man was arrested March 28 on suspicion of pilfering firefighting equipment from California's Contra Costa Fire District's annexes over the span of a year, investigators said. The Concord resident has been linked to a series of thefts that surfaced July 2011 when someone was seen climbing a fence at the fire district's training center. That particular break-in remained unsolved until February after an audit revealed the disappearance of various items, including breathing units, axes, sledgehammers, and even a chain saw, sparking an investigation involving fire investigators and Concord police. Investigators canvassed the sprawling training center and found multiple breaches in the fencing. Investigators began surveillance operations and on several occasions they recorded the suspect on the property. That became the basis of a felony arrest warrant obtained by Concord police.
Source: http://www.mercurynews.com/news/ci_20281929/man-arrested-serial-thefts-from-contra-costa-fire

For another story, see item **31**

[Return to top]

Information Technology Sector

39. *April 2, H Security* – (International) **Rails 3.2.3 makes mass assignment change.** The Ruby on Rails developers published Rails 3.2.3 which includes the mass assignment change that appeared in the wake of March's GitHub incident. In that incident, a developer used a well-known vulnerability in the default configuration of Rails applications to manipulate GitHub projects. The problem was that, for ease of development, Rails allowed any field in a database record to be set in a mass assignment action and then left it to the developer to lock down the application. The change in Rails 3.2.3 now forces developers to whitelist fields for mass assignment by flipping the config.active_record.whitelist_attributes property to true by default. This change only affects new applications and developers should check their existing Rails applications for mass assignment vulnerabilities or to set the

config.active_record.whitelist_attributes property to true in their applications. The 3.2.3 release also sees the addition of an option to change to how authenticity_tokens are handled when doing remote forms, and an update to rack-cache (to fix a cookie leak) and mail to address security vulnerabilities.
Source: http://www.h-online.com/security/news/item/Rails-3-2-3-makes-mass-assignment-change-1498547.html

40. *April 2, The Register* – (International) **Pastebin.com hiring staff to get rid of activists' dumps.** Pastebin.com has promised to police content on its site more tightly by hiring staff to delete data dumps and other sensitive information more quickly. The site, one of several of its type and originally set up primarily for programmers, has become a favorite dumping ground for hacktivists from Anonymous and LulzSec over recent months. Many of these posts revealed an array of personal information swiped from the insecure systems of targets including home addresses, e-mail passwords, and credit card details. The dumps are then linked to and publicized by Twitter updates from the various hacktivists.
Source: http://www.theregister.co.uk/2012/04/02/pastebin_content_policing/

41. *April 2, H Security* – (International) **Security vulnerability at TweetDeck.** The TweetDeck Twitter client apparently suffered from a security breach March 30 that gave some users the ability to take over other people's accounts. Twitter, which owns TweetDeck, reacted quickly and disabled the client's access to the system. TweetDeck's functionality was restored less than a day later, once the bug was fixed. A TweetDeck user discovered the bug which gave him access to the Twitter and Facebook accounts of hundreds of other TweetDeck users. TweetDeck allows its users to pull together both Twitter and Facebook accounts under a TweetDeck account to aggregate updates from both services. The user publicly reported the problem on Twitter, posting a screenshot to document the vulnerability. To back up his claims, he also posted several messages from other people's accounts. In a statement to VentureBeat and other U.S. media, Twitter representatives said no account passwords were compromised and , as far as Twitter is aware, the vulnerability was not exploited maliciously. Facebook told the Wall Street Journal that fewer than 250 of its users were affected, no abuse of those accounts occurred, and it was working with Twitter to "understand the full scope of this issue."
Source: http://www.h-online.com/security/news/item/Security-vulnerability-at-TweetDeck-1498585.html

42. *April 2, The Register* – (International) **Mac Java hole exploited by wild Flashback trojan strain.** Security watchers have discovered a strain of Mac-specific malware that exploits an unpatched vulnerability in Java. A variant of the Flashback trojan exploiting CVE-2012-0507 (a Java vulnerability) was spotted in the wild, F-Secure warns. Oracle patched the vulnerability for Windows machines in February, but has yet to issue a fix for Mac OS X — creating a window of opportunity for virus writers. F-Secure advises users to disable Java, which is not needed to visit the vast majority of Web sites, on their Mac. Some banking Web sites mandate the use of Java, in which case security-conscious Mac users can re-enable Java for the duration of their session before turning

it off again, the security firm suggests.
Source: http://www.theregister.co.uk/2012/04/02/flashback_mac_malware/

43. *April 2, Help Net Security* – (International) **Potential first Android bootkit spotted.** Security researchers of NQ Mobile recently discovered what might be the first Android bootkit. Dubbed DKFBootKit, the malware piggybacks malicious payloads into legitimate apps that require root privilege. "Specifically, by taking advantage of the root privilege, DKFBootKit adds itself as a part of the boot sequence of the original Android system and replaces a number of utility programs (e.g., ifconfig and mount)," claim the researchers. "By doing so, the malware can get started even before the entire Android framework is bootstrapped." The apps targeted for repackaging with the malicious payload are mostly utility apps, but a few are also apps that provide license keys for some paid apps. The malware's final goal is to make itself run earlier than the Android framework, and to deliver a bot payload that connects the device to several command and control servers and waits to receive additional commands.
Source: http://www.net-security.org/malware_news.php?id=2051&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

44. *March 31, Softpedia* – (International) **Expert shows how hackers can use CSRF browser vulnerability.** The hacker who broke into GitHub to demonstrate a vulnerability warns that cross-site request forgery (CSRF), a security hole that affects all browsers, must be addressed immediately because it poses a great risk for unsuspecting users. He claims CSRF security holes have been present for a long time, but many underestimated the dangers hiding behind them. Unlike cross-site scripting attacks which exploit the trust of a user towards a particular site, CSRF attacks rely on the trust that a site has in a browser. The expert explains that when users sign in to any site, dubbed by the researcher as site1.com, they are remembered by the cookie mechanism. By leveraging the vulnerability, the hacker can shorten the Web site's session and social engineer the victim into signing in again. The user signs in the second time and a malicious script is triggered. Then, when the user visits a second site, named site2.com, the exploit begins.
Source: http://news.softpedia.com/news/Expert-Shows-How-Hackers-Can-Use-CSRF-Browser-Vulnerability-262109.shtml

For more stories, see items **2**, **7**, and **10**

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 1, KNDU 25 Kennewick; KNDO 23 Yakima* – (Washington) **Local radio station hijacked.** The radio station Power 99.1 KUJ FM in Burbank, Washington, has been having their signal hijacked, KNDU 25 Kennewick and KNDO 23 Yakima reported April 1. The hijacker called himself the radio pirate and is breaking onto the airwaves making small statements and playing his choice of songs. The hijackings started March 28 and each day there were a few instances of piracy. The station was working with the Federal Communications Commission and local law enforcement to solve the case.
Source: http://www.kndo.com/story/17307068/local-radio-station-hijacked

[Return to top]

Commercial Facilities Sector

46. *April 2, Softpedia* – (National) **PBS website hacked by Anonymous, passwords dumped.** Anonymous hackers claimed to have breached the Web site of the Public Broadcasting Service (pbs.org), leaking large amounts of sensitive information from its databases, Softpedia reported April 2. One of the dump files, published on Pastebin, contained around 300 usernames and password hashes that can allegedly be used to access the site's database. Another post held close to 200 record sets that represent "stations and password." It was uncertain as of April 2 what the passwords access, but the file also contained TV station names, Web site URLs, e-mail addresses, physical addresses, and contact details. A number of 1,600 usernames, clear-text passwords, and e-mail addresses that belong to the members of the press were also leaked. A separate file showed the usernames, names, e-mail addresses, and password hashes of Web site administrators, totaling a number of 38 records, and another one, entitled "logins" held 250 names, usernames, e-mail addresses, and passwords. The site was previously hacked two times in 2011.
Source: http://news.softpedia.com/news/PBS-Website-Hacked-by-Anonymous-Passwords-Dumped-262195.shtml

47. *April 1, The Bergen County Record* – (New Jersey) **Ridgewood building evacuated for fumes.** Firefighters evacuated a five-story office building in Ridgewood, New Jersey, April 1 following reports of a sulfuric acid odor coming from the basement. A leak caused by a malfunctioning battery used to support cell phone towers located in the building was the cause of the odors. Tenants of the Lincoln Building, were kept out for 2 hours as the Bergen County Hazardous Materials unit investigated. Six people were medically evaluated on the scene, but no one required additional medical treatment. A fire captain said carbon monoxide levels were elevated in the building. The fire crews ventilated the building with power fans until HAZMAT investigators determined it was safe to occupy.
Source:

http://www.northjersey.com/news/bergen/bergen_safety/Ridgewood_commercial_building_evacuated_.html

48. *April 1, Arizona Republic News; KPNX 12 Phoenix* – (Arizona) **Blaze guts Mesa strip mall.** It took more than 60 firefighters from 4 departments to get the upper hand on a fire that engulfed a Mesa, Arizona strip mall April 1. When the fire was extinguished, only 1 of 10 businesses was saved at the the Granite Reef Plaza shopping center. One Mesa police officer who responded suffered smoke inhalation and was taken to a medical center. Smoke was so intense that homes north of the strip mall had to be evacuated. The fire broke out in one of the units and "spread very quickly from there," a fire department spokesman said. Investigators were looking into the cause of the fire.
Source: http://www.azcentral.com/community/mesa/articles/2012/04/01/20120401blaze-guts-mesa-strip-mall.html

49. *March 31, CNN* – (Florida) **2 killed, 12 injured in mass shooting during funeral in Miami.** Two people were killed and 12 injured after a shooting outside a Miami funeral home March 30, police said. Investigators from the Miami-Dade County Police Department's homicide bureau continued their probe March 31, a day after the mass shooting took place. The shooting occurred at the Monique and Loriston Community Funeral Home in north Miami, "while funeral services were taking place," according to a press release issued by police.
Source: http://www.cnn.com/2012/03/31/us/florida-funeral-shooting/index.html?hpt=us_c2

50. *March 31, KCPQ 13 Seattle* – (Washington) **Low visibility halts search for 2 missing after Bellingham boathouse fire.** Two people were unaccounted for after a fire destroyed a boathouse in Bellingham, Washington, March 30. The boathouse, which can hold up to 20 boats, was fully engulfed in flames early March 30. The U.S. Coast Guard also responded to the scene of the fire to investigate any possible water contamination and to assist fire crews. The Washington Department of Ecology was on the scene to help assess environmental damage and oversee cleanup operations from the fire. Emergency response crews continued to search for two missing people who were living aboard their boat in the boathouse. However, adverse weather conditions during the weekend of March 31 prevented divers from searching for the missing people.
Source: http://www.q13fox.com/news/kcpq-bellingham-dock-fire-20120330,0,1137046.story?track=rss

51. *March 30, KRIV 26 Houston* – (Texas) **Police discover dead man, evidence of bomb inside Mont Belvieu apartment.** Following the evacuation of a Mont Belvieu, Texas apartment complex March 30, a bomb squad discovered wired explosives, chemicals, and gunpowder in the apartment of a dead man. Police were called to a man's apartment after the man's employer called police to check on him. When officers entered the apartment, they found the man dead, apparently of natural causes. While taking the body away, emergency crews discovered a number of weapons and information on anti-government activities and bomb making. The Alcohol, Tobacco,

and Firearms Bureau was alerted as a result. Bomb squads were sent to the scene, and police evacuated nearly half of the complex surrounding the man's apartment. The bomb squad found explosives resembling homemade improvised explosive devices. The search for those devices proved difficult as it seemed the dead man was a hoarder. Crews had to clear the hoarded material as they searched.
Source: http://www.myfoxhouston.com/dpp/news/local/120330-apartments-evacuated-bomb-squads-searching-home

For another story, see item **9**

[Return to top]

National Monuments and Icons Sector

52. *April 2, KMGH 7 Denver* – (Colorado) **Lower North Fork Fire evacuees go back home.** Authorities allowed all remaining evacuees from the Lower North Fork wildfire in Colorado to return home April 2. A representative of the Jefferson County Sheriff's Office said that residents of the last 50 homes were allowed to return April 2, nearly a week after the fire erupted. All roads in the burn area, with the exception of Kuehster Road, have reopened to the public. Kuehster Road will remain open only to residents until further notice. The representative said firefighters had contained 97 percent of the fire's perimeter. At its peak, the blaze forced mandatory evacuations of 900 homes and left even more families on standby. More than two dozen homes were damaged or destroyed. Colorado has suspended controlled burns that are designed to reduce wildfire risk after the Colorado State Forest Service acknowledged that a March 22 prescribed burn may have rekindled and triggered the North Fork Fire. High wind gusts blew embers across a containment line, the forest service said. Utilities are slowly being restored inside the fire zone. Electricity and natural gas crews are working with emergency officials to restore services in much of the area.
Source: http://www.thedenverchannel.com/news/30816519/detail.html

53. *April 1, Associated Press* – (South Dakota) **SD forest fire contained.** Officials said the Black Hills National Forest fire in southwest South Dakota has been contained. The Forest Service said the fire was contained March 31, after scorching 546 acres. The agency said no structures were threatened and no injuries were reported in the Apple Fire, which was started by lightning March 28.
Source: http://hosted2.ap.org/ALDEC/TDNational/Article_2012-04-01-SD%20Forest%20Fire/id-9f5b1e286e3b4871b9f6862f518cd4cc

54. *March 31, Associated Press* – (Texas) **Texas firefighter charged with setting wildfire.** A volunteer firefighter in Texas was charged with setting a wildfire in 2011. The man was charged with arson, a second-degree felony, in connection with a May 2011 wildfire in Jones County. The 24-year-old was a lieutenant with the Hamby Volunteer Fire Department, just outside Abilene. The Texas Forest Service said it began investigating the man after he was recently charged with first-degree arson. He was arrested the week of March 26 after a fire at Hamby United Methodist Church. He remained jailed in Taylor County on $110,000 bond.

Source: http://www.ksat.com/news/Texas-firefighter-charged-with-setting-wildfire/-/478452/9915726/-/q4dqb8/-/index.html

[Return to top]

Dams Sector

55. *March 31, Baxter Bulletin* – (Arkansas) **Corps increases releases from White River Basin lakes.** The Army Corps of Engineers Little Rock District in Arkansas increased releases from its White River Basin lakes to lower lake levels after the heavy rains during March. Releases as of March 29 were: Table Rock Dam, 14,000 cubic feet per second (cfs) ; Bull Shoals Dam, 22,000 cfs; Norfork Dam, 6,000 cfs; and Greers Ferry Dam, 6,500 cfs. The White River system operating plan calls for the Corps to regulate up to a 24-foot river stage at Newport and up to a 22-foot stage at Georgetown until April 14. It allows the Corps to evacuate more flood storage now before moving into April and May, historically the most flood prone months. Since they were constructed, the White River Basin lakes and levees have prevented more than $1 billion in flood losses. Increased releases from Beaver Dam are forecast to begin in mid-April, barring additional heavy rain.
Source: http://www.baxterbulletin.com/article/20120401/NEWS01/120331006/Corps-increases-releases-from-White-River-Basin-lakes

56. *March 29, New York Times* – (New Jersey; National) **Flooding risk rises statewide.** A new study by the nonprofit Climate Central in Princeton, New Jersey, investigated the threat that rising seas pose to coastal communities. It found that among states with municipalities at elevated risk of severe flooding, New Jersey was tied for third place with North Carolina, the New York Times reported March 29. Inland, towns along the Raritan, Passaic, and Delaware Rivers have recently been walloped by a series of intense storms that left thousands of home and business owners reeling. The increased frequency of these flood-causing events has scientists wondering if this is the “new normal” for New Jersey, while public officials, engineers, and insurance companies grapple with how to respond. The study of rising sea levels and an accompanying report, “Surging Seas,” predict that the ocean could rise a foot over the next 30 to 40 years, increasing the vulnerability of the 3.7 million Americans living less than four feet above sea level. Like North Carolina, New Jersey has 22 municipalities in which more than half the population lives below the 4-foot mark, according to the study. Florida has 106 such communities, Louisiana 65. The study includes an interactive map that outlines the threat levels to 3,000 coastal areas.
Source: http://www.nytimes.com/2012/04/01/realestate/new-jersey-in-the-region-flooding-risk-rises-statewide.html?_r=1

[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