Daily Open Source Infrastructure Report
2 April 2012

Top Stories

- An audit revealed that more than $7 million in taxpayer-purchased fuels for Los Angeles city vehicles has gone unaccounted for in recent years. – *Los Angeles Times* (See item **2**)
- Global Payments Inc, an Atlanta-based payments processor, was broken into by hackers, leaving more than 50,000 Visa and MasterCard accounts potentially compromised, according to news reports March 30. – *Wired* (See item **11**)
- Colorado authorities investigated problems with an emergency notification system March 30 because some residents who signed up never got a warning about a dangerous wildfire. Two people were killed in the fire and more than 900 homes were evacuated. – *Associated Press* (See item **40**)
- Scrap metal thieves targeting fiber optic cables shut down 9-1-1 service in Ohio's Appalachian region and left thousands of residents, banks, and other businesses without telephone and Internet services. – *Associated Press* (See item **48**)

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. *March 30, Scranton Times-Tribune* – (Pennsylvania) **Explosion rocks natural gas compressor station.** An explosion at a natural gas compressor station in Susquehanna County, Pennsylvania, March 29, blew a hole in the roof of the complex holding the engines, shaking homes as far as a half-mile away and drawing emergency responders from nearby counties. The blast at the Lathrop Township station off Route 29 sent black and gray clouds billowing from the building for several hours, but the damage was contained to the site, said a spokeswoman for Williams Partners LP, which owns the station. Automated emergency shutdown procedures stopped gas from entering or leaving the compressors, and Williams will do a full investigation of the cause and damage. The Lathrop station pressurizes and dehydrates natural gas from Marcellus Shale wells in the county for transport through interstate pipelines, including the Tennessee and Transco, which bring the gas to market.
Source: http://thetimes-tribune.com/news/explosion-rocks-natural-gas-compressor-station-1.1292502#axzz1qbtkvUNt

2. *March 30, Los Angeles Times* – (California) **L.A. officials were warned in 2009 of gaps in tracking of fuel.** Los Angeles city officials were warned by auditors 3 years ago about gaps in the way the city tracks millions of gallons of taxpayer-purchased fuel. However, according to a new audit released March 29 by the city controller, not enough was done to fix the problems. The audit highlights that more than $7 million in gasoline and other fuels has gone unaccounted for in recent years. Each year, Los Angeles spends close to $29 million on 14 million gallons of gasoline, natural gas, and diesel fuel to run garbage trucks, helicopters, police cruisers, and other vehicles. Every transaction is supposed to be tracked, manually or electronically. However, there are ways to bypass tracking systems. Bypass mechanisms are supposed to be employed only when normal systems fail, but auditors found they were used to dispense millions of gallons of fuel over a 22-month period beginning in 2009. The unexplained transactions occurred despite a $12-million fuel-tracking system and accountability measures put in place after a 2009 audit. During the course of the 2009 audit, general services established a task force to address the fuel-tracking problems and develop the Web site. However, few departments actually monitor the online reports. With more oversight, an auditor said, the unexplained transactions might have been caught sooner.
Source: http://www.latimes.com/news/local/la-me-0330-missing-fuel-20120330,0,7891840.story

3. *March 29, Reuters* – (International) **Mexico's Pemex signs deep water oil drilling safety contract.** Mexico's state oil monopoly Pemex signed a contract with a company specializing in oil spill clean ups to boost its safety controls as it plunges into exploration of deep waters in the Gulf of Mexico. Pemex said in a statement March 29 that Wild Well Control, which was heavily involved in efforts to cap a leaking well in the wake of BP's Deepwater Horizon disaster in 2010, will help Pemex comply with

rules put in place by the country's oil watchdog the National Hydrocarbons Commision (CNH). Pemex has limited experience in deep water drilling but estimates there are more than 29 billion barrels of crude equivalent, or 58 percent of the country's prospective resources, in the Gulf. The CNH is concerned Mexico on its own is not ready to take on ultra-deep projects like the Maximino well, which is planned for 2013 at around 10,000 feet, 6 times deeper than Pemex has drilled before.
Source: http://www.reuters.com/article/2012/03/30/mexico-oil-idUSL2E8EU0WX20120330

For another story, see item **52**

[Return to top]

Chemical Industry Sector

4. *March 29, Provo Daily Herald* – (Utah) **Orem fuel company engulfed in chemical fire.** A comb of black smoke arched above Orem, Utah, March 29 after a chemical fire burst out at a company that makes fuel additives. The Orem fire inspector said workers were pumping fuel when malfunctioning equipment sprayed flammable liquid on a hot pump. The liquid then ignited. Crews from Orem and Provo responded and had the blaze under control quickly. Damage to the building was limited due to its cinder block construction, the fire inspector said, though the fire did spread to the wooden roof and rafters. He estimated damage to be around $300,000. More than an hour after the fire ignited, smoke continued to stream out of vents in the roof and firefighters used a chain saw to cut access holes.
Source: http://www.heraldextra.com/news/local/central/orem/orem-fuel-company-engulfed-in-chemical-fire/article_8f8e22f6-79d0-11e1-bcfa-0019bb2963f4.html

5. *March 28, WVLA 33 Baton Rouge* – (Louisiana) **Hazmat situation in Donaldsonville sends at least one to hospital.** A HAZMAT situation at CF Industries Nitrogen Complex in Donaldsonville, Louisiana, shut down LA 18 north at LA 3120 March 28. The plant manager said they started a shutdown of one of their ammonia plants to avoid a failure. During that shut down, a chemical called amine was released into the air. A person driving by the plant at the time was momentarily blinded by the chemical and crashed his vehicle on plant property. He was taken to a local hospital. Plant officials said they would clean up the spill. Louisiana environmental officials were monitoring the situation.
Source: http://www.nbc33tv.com/news/local-news/hazmat-situation-in-donaldsonville-sends-at-least-one-to-hospital

For more stories, see items **26**, **29**, and **46**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

6. *March 30, Reuters* – (National) **Honda recalls 554,000 SUVs over headlights.** Honda Motor Co Ltd, March 30, announced the recall of about 554,000 sport utility vehicles in the United States to inspect for faulty wiring in headlights. Honda said in a statement that the recall affects CR-V SUVs from model years 2002 to 2004 and Pilot SUVs from model year 2003. The automaker will inspect and replace parts of the headlight wiring system that could fail, causing the low-beam headlights not to work and increase the risk of crash.
   Source: http://news.yahoo.com/honda-recalls-554-000-suvs-over-headlights-111306046.html

7. *March 29, Associated Press* – (Missouri) **Doe Run: Fire caused significant damage at smelter.** The Doe Run Co. said production of primary lead at its smelter in Herculaneum, Missouri, will be suspended for 4 to 6 weeks following a fire, the Associated Press reported March 29. The March 20 fire occurred at the smelter's electric substation. Doe Run Primary Smelting Division's general manager said damage to the substation was significant. The company said it has contacted customers to advise them of the halt in production.
   Source: http://www.ksdk.com/news/article/312992/3/Doe-Run-Fire-caused-significant-damage-at-smelter

8. *March 29, U.S. Department of Labor* – (Ohio) **U.S. Department of Labor's OSHA cites Findlay, Ohio-based Sanoh America with 13 safety violations for exposing workers to fire, other hazards.** The U.S. Department of Labor's Occupational Safety and Health Administration cited auto parts manufacturer Sanoh America Inc. March 29 with 13 violations, including one repeat, for exposing workers to fire hazards, dangerous fumes, and other safety hazards at the company's Findlay, Ohio plant. An October 4, 2011, inspection — initiated based on a complaint — determined the facility's plating line had caught fire during production earlier in the year. A repeat violation and 12 serious violations were cited.
   Source:
   http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22074

9. *March 29, Watertown Daily Times* – (New York) **Alcoa: Fire is under control.** Alcoa officials said there were no injuries when an aluminum chip melter malfunctioned at the Alcoa West plant in Messena, New York, March 29. A fire at the casthouse was declared under control, though firefighters remained on the scene and battled hot spots. No hazardous materials were in the area where the melter malfunctioned, sparking the blaze. An Alcoa spokeswoman said the cast house and the nearby extrusion building — facilities in the center of the plant — were evacuated. Alcoa told its midnight shift at the casthouse that they did not need to report for work the night of March 29, and the

day shift was told to report to the clubhouse the morning of March 30.
Source: http://www.watertowndailytimes.com/article/20120329/NEWS09/703309973

[Return to top]

Defense Industrial Base Sector

10. *March 29, Associated Press* – (National) **Oxygen problem in F-22 Raptor remains a mystery.** A U.S. Air Force advisory panel said it still cannot explain what caused blackouts and dizziness among pilots flying its supersonic F-22 Raptor. Officials told a Pentagon press conference March 29 that the stealth fighter is safe and continues to fly in the continental United States, with pilots using special sensors, filters, and other safety steps to mitigate problems with the plane's on-board oxygen system. The Air Force said it is putting into place a number of safety recommendations made in the 7-month study. The head of the study panel said officials will continue to investigate the problem until they find its cause. The Air Force's entire fleet of those fighters, which are made by Lockheed Martin Corp., was grounded for 4 months in 2011 until mid-September after pilots complained of lack of oxygen.
Source: http://www.sacbee.com/2012/03/29/4376857/oxygen-problem-in-f-22-raptor.html

For another story, see item **46**

[Return to top]

Banking and Finance Sector

11. *March 30, Wired* – (International) **Hackers breach credit card processor; 50K cards compromised.** Global Payments Inc, an Atlanta-based payments processor, was broken into by hackers, leaving more than 50,000 card accounts potentially compromised, according to news reports March 30. The breach occurred sometime between January 21 and February 25 according to notices that Visa and MasterCard sent to banks recently. The extent of the breach and damages are still unknown, but it appears to be rather small based on initial reports from the Wall Street Journal and elsewhere. A notice sent by credit union service organization PSCU to its customers indicated Visa alerted it March 23 that 46,194 Visa accounts might have been compromised. However, that number was downgraded to just 26,000 after eliminating duplicate account numbers and cards with invalid expiration dates, according to the Journal. Only about 800 accounts are known to have had fraudulent activity on them so far, according to a security blogger who broke the story and reported that Track 1 and Track 2 data had been taken, making it easy for criminals to clone the cards and use them for fraudulent activity. The number of accounts showing fraudulent activity could rise, however, as the investigation continues.
Source: http://www.wired.com/threatlevel/2012/03/global-payments-breached/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+%28Wired:+Index+3+%28Top+Stories+2%29%29&utm_content=Google+Reader%20%3Chttp:%20www.wired.com

12. *March 30, Aspen Daily News* – (Colorado; National; International) **Local credit-card fraud cases reach into the hundreds.** The number of credit-card fraud cases reported to the Aspen, Colorado Police Department (APD) surpassed more than 100 within in a month's time, and local law enforcement is now working with the Secret Service and the FBI to solve the crimes, the Aspen Daily News reported March 30. There are likely more instances than that, as many banking customers have not reported their cards being compromised to police or the sheriff's office, the latter of which is reporting 20 active cases. In many instances, the bank informs customers their debit or credit-card numbers have been run in other cities across the country without their authorization; some have been charged outside the United States. In response, area banks have issued hundreds of new debit and credit cards. Several city employees' purchasing cards have been compromised in the past month as well. The APD also is working with senior investigators at merchant service companies, which process credit and debit cards, to find a common thread to see where charges may have originated. Local police thus far have not been able to determine a connection between the cases, which appear to be originating from Aspen.
Source: http://www.aspendailynews.com/section/home/152518

13. *March 30, WRAL 5 Raleigh* – (North Carolina) **Cary police arrest two men accused of using fake credit cards.** Police in Cary, North Carolina, arrested two men March 29 at Cary Town Mall accused of using counterfeit credit cards to make purchases at various department stores over the last 3 weeks. Police said the pair admitted to using the fake credit cards to purchase clothing, electronics, and other items. Officers recovered more than 100 counterfeit cards in their possession. The man are charged with felony conspiracy, possession of a counterfeit instrument, obtaining property by false pretenses, and unlawfully obtaining credit cards.
Source: http://www.wral.com/news/news_briefs/story/10925125/

14. *March 29, U.S. Department of Justice* – (California) **Federal court permanently bars San Diego accountant from preparing tax returns that understate income.** A federal court has permanently barred a certified public accountant from San Diego from providing tax advice or preparing federal tax returns that illegally attempt to reduce customers' taxable income, the Justice Department announced March 29. The order also bars him from providing tax advice to, or preparing the federal tax returns of, any individual or entity that he knows is a customer of his co-defendant. The government complaint in the case alleged the man worked with his co-defendant, a San Diego tax lawyer, to help clients evade income taxes and illegally circumvent pension plan rules. According to the civil injunction suit, the co-defendant promoted schemes that helped customers evade taxes through the use of bogus deductions, while the accountant prepared the customers' tax returns. The government alleged that the Internal Revenue Service audited more than 1,000 tax returns as a result of the pair's alleged tax schemes, and it estimated that the harm to the U.S. Treasury from the schemes exceeded $10.8 million.
Source: http://www.justice.gov/tax/2012/txdv12400.htm

15. *March 29, U.S. Department of Justice* – (Indiana) **Justice Department asks federal court to bar Indiana firm from preparing tax returns.** The United States has asked a

federal court to bar a tax preparation firm and its owner from preparing tax returns for others, the Justice Department announced March 29. According to the complaint, the owner's business, Quick Sam Tax Refund of Gary, Indiana, has repeatedly prepared tax returns that unlawfully understate customers' income tax liabilities by fabricating expenses, creating false losses, and claiming bogus dependents. According to the complaint, Quick Sam guarantees its customers they will receive the largest refund by getting their taxes prepared at Quick Sam. To deliver on this promise, the complaint alleges Quick Sam employees fabricate business expenses, claim improper tax credits, and report fictitious dependents to increase customers' tax refunds illegally. The owner and Quick Sam allegedly give bonuses to employees for engaging in these fraudulent practices. The complaint said that over 96 percent of Quick Sam returns examined by the Internal Revenue Service (IRS) contained deficiencies requiring IRS adjustments. The complaint alleges the total harm to the government caused by the illegal conduct could exceed $35 million. The complaint also states that four former Quick Sam return preparers have recently pleaded guilty to tax-related crimes.
Source: http://www.justice.gov/tax/2012/txdv12401.htm

16. *March 28, U.S. Federal Trade Commission* – (National) **FTC takes action against bogus precious metals investment scheme.** The U.S. Federal Trade Commission (FTC) has taken action to halt a telemarketing operation that allegedly took millions of dollars from senior citizens by conning them into buying precious metals on credit without clearly disclosing significant costs and risks, including the likelihood that consumers would subsequently have to pay more money or lose their investment, according to a March 28 press release. According to the FTC filing, the operation has taken in almost $9 million from consumers in the past 2 years. The court ordered a stop to the defendants' allegedly deceptive practices pending a hearing, froze their assets, and appointed a receiver to oversee the business. The FTC charged Premier Precious Metals Inc., Rushmore Consulting Group Inc., PPM Credit Inc., and the companies' principal and owner promised consumers they could earn large profits quickly and safely by investing in precious metals. Allegedly using high-pressure sales tactics, telemarketers told consumers they were offering lucrative investments certain to earn consumers significant profits, with very little risk of loss. However, the leveraged investments were typically not profitable and carried a high risk of loss. As alleged in the FTC complaint, the defendants did not clearly disclose the total costs of investments, including the hefty fees, commission, and interest charges consumers had to pay to buy and maintain the investments.
Source: http://www.ftc.gov/opa/2012/03/preciousmetals.shtm

For another story, see item **48**

[Return to top]

Transportation Sector

17. *March 30, Palm Beach Post* – (Florida) **Local, state, and federal agencies to meet on fatal school bus crash in St. Lucie.** State, local, and federal investigators in Florida were expected to meet March 30 to discuss the March 26 school bus crash in Fort

Pierce that left a boy dead and sent more than a dozen other children to area hospitals, a Florida Highway Patrol (FHP) sergeant said March 29. Officials from the FHP, St. Lucie County Sheriff's Office, and National Transportation Safety Board (NTSB) were expected to meet in Fort Pierce to complete a crash report and an in-depth traffic fatality report. The five children injured in the crash remained hospitalized March 30 in West Palm Beach. At least one of those children sustained a brain injury. NTSB officials will look at the crash as part of broader efforts to make school buses safer on a national level, said a NTSB public affairs officer. The agency will examine all aspects of the vehicles, drivers, and environmental factors involved. The bus, which had been traveling west, was struck by an eastbound semitrailer hauling sod after the bus turned left in front of it, according to the FHP.
Source: http://www.palmbeachpost.com/news/local-state-and-federal-agencies-to-meet-on-2271621.html

18. *March 30, Associated Press* – (Rhode Island) **Amtrak train delayed as wheels leave track in RI.** An Amtrak train was traveling from Boston to Washington D.C. when its front wheels came off the tracks in North Kingstown, Rhode Island, March 29. Amtrak officials told WLNE 6 Providence that the 265 passengers on the Acela train were delayed for about half an hour until another train picked them up. There were no injuries, and a crane was brought in to lift the train back onto its tracks. It was unclear what caused the train to come off its tracks.
Source: http://abcnews.go.com/US/wireStory/amtrak-train-delayed-wheels-leave-track-ri-16036349#.T3W2VtnW6F8

19. *March 30, Mid-Hudson News* – (New York) **Port Authority to centralize security operations.** The Port Authority of New York and New Jersey approved a new standalone security department to direct all elements related to agency security matters, Mid-Hudson News reported March 30. The new agency will assume full operational control of the Port Authority Police Department. A board chairman said the new department will enhance security operations and will hire a chief security officer. The announcement of the new department came after a private briefing of the Port Board by a former U.S. Homeland Security Secretary. His security consulting was hired by the Port Authority in May 2011 to perform a top-to-bottom study of the authority's management of security and agency-wide security operations.
Source: http://www.midhudsonnews.com/News/2012/March/30/PA_sec-30Mar12.html

For more stories, see items **1**, **5**, **30**, and **31**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

20. *March 30, Food Safety News* – (Illinois; Michigan) **Listeria tests prompt recall of halal 'Kubba' beef.** Mosul Kubba of Chicago is recalling approximately 1,100 pounds of stuffed, layered beef products due to possible contamination with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced March 29. The problem was discovered during routine FSIS testing. The fully cooked, ready-to-eat, halal beef products were produced March 20 and then shipped to a single distributor in Detroit.
Source: http://www.foodsafetynews.com/2012/03/listeria-tests-prompt-recall-of-halal-kubba-beef/

21. *March 30, Food Safety News* – (Illinois; Michigan; Ohio) **Allergen alert: Cookies with milk.** Topnotch Cookies & Cakes of Westland, Michigan, is recalling certain chocolate chip cookies because they may contain undeclared traces of milk, an allergen, in the butter and vanilla flavoring, Food Safety News reported March 30. The recall was initiated after it was discovered the supplier of the flavoring had added milk product, which was not listed among the ingredients. The problem has been corrected. â□¨The recalled cookies were distributed in Detroit and Lansing, Michigan; Cleveland; and Chicago to retail stores.
Source: http://www.foodsafetynews.com/2012/03/allergen-alert-cookies-with-milk-1/

22. *March 30, Food Safety News* – (California) **California lifts quarantine on Claravale Farm raw milk.** The California State veterinarian lifted a statewide quarantine March 29 on raw milk produced by Claravale Farm, while the state department of public health said it is still conducting an epidemiological investigation of reported clusters of Campylobacter infection associated with consumption of unpasteurized milk products. In a news release, the California Department of Food and Agriculture (CDFA) said Claravale has met state sanitation requirements and food safety regulations to clear its production, processing, and packaging operations, which were temporarily halted March 23 after CDFA tests detected Campylobacter in the dairy's raw cream. The CDFA then issued a recall and quarantine hold of Claravale products.
Source: http://www.foodsafetynews.com/2012/03/california-lifts-quarantine-on-claravale-farm-raw-milk/

23. *March 30, Food Safety News* – (California) **FDA seeks to stop CA fish producer, cites botulism risk.** The U.S. Food and Drug Administration (FDA) is seeking an injunction against a California seafood company because of a risk of botulism and other food hazards in its fish and fish products, Food Safety News reported March 30. Government inspections found Fujino Enterprises Inc., which operates under the name Blue Ocean Smokehouse, was not meeting sanitation guidelines for seafood production, thus leaving room for potential botulism contamination and other hazards. After the firm failed to update its practices, FDA filed a complaint seeking to shut down fish processing and distribution at the plant. Blue Ocean processes fresh and smoked fish and fish products, including salmon, cod, halibut, Wild King Salmon Candy, hot-smoked tuna, sturgeon, and hot-smoked fish cream cheese spreads. The firm's hot and cold smoked fish products are processed in a way that may allow for the

growth of Clostridium botulinum, a toxin that can cause paralysis, respiratory problems, and death, the FDA said. Its tuna products were found to be at risk for the development of scombrotoxin, which causes symptoms similar to those of an allergic reaction, including difficulty breathing, headache, nausea, and abdominal cramps. Inspections also revealed Listeria monocytogenes bacteria on food-contact and non-food-contact surfaces in food processing areas. Blue Ocean voluntarily destroyed nearly 1,500 pounds of hot- and cold-smoked fish in October 2011 under the supervision of the FDA and the California Department of Health.
Source: http://www.foodsafetynews.com/2012/03/fda-seeks-to-stop-ca-fish-producer-cites-botulism-risk/

24. *March 30, Food Safety News* – (National) **No sign of oyster recovery two years after BP oil spill.** With the second anniversary of the BP oil spill approaching, attention is once again returning to the damaged Gulf of Mexico environment, especially to its greatly diminished oyster production, Food Safety News reported March 30. The worst man-made environmental disaster in U.S. history put 200 million gallons of oil and 2 million gallons of toxic dispersants into the waters of the Gulf with the April 20, 2010 explosion of BP's Deepwater Horizon drilling platform and uncontrolled oil spill it caused. The Gulf oyster supply is going through a second very limited season with demand not reaching anywhere near pre-BP oil spill levels. BP has not yet had to pay a dime in compensation for its impact on the Gulf ecosystem. The federal government could pursue criminal environmental penalties and separate civil action against BP, which together might hit $60 billion.
Source: http://www.foodsafetynews.com/2012/03/no-sign-of-oyster-recovery-two-years-after-bp-oil-spill/

25. *March 29, Food Safety News* – (National) **FSIS issues new trim sampling requirements.** The USDA's Food Safety & Inspection Service (FSIS) issued a notice the week of March 19 that gives its inspection personnel specific instructions on how to randomly select the beef trimmings to be tested under the MT50 project code, which includes E. coli testing in trim. The notice instructs inspectors to collect samples from all types of trim if a plant is producing multiple types. Previously, inspectors were only required to collect samples for one type of trim. The notice also has instructions for sampling ammoniated beef. Inspectors "are not to combine samples from two piece chucks with source materials designated for anhydrous ammonia treatment. The intent is that, through random selection, all products that fall under the beef manufacturing trim sampling program will likely be selected over time." FSIS samples beef manufacturing trimmings at the slaughter establishment. Inspectors then submit information on the type of trim collected through the Public Health Information System.
Source: http://www.foodsafetynews.com/2012/03/fsis-issues-new-trim-sampling-requirements/

26. *March 29, Chicago Sun-Times* – (Illinois) **Chicago meat processor plant draws $118,700 OSHA fines.** A California-based food company was accused of 22 safety and health violations at its meat processing plant in Chicago and faces penalties of up to $118,700, the Chicago Sun-Times reported March 29. The U.S. Occupational Safety

and Health Administration (OSHA) began an inspection September 29, 2011 at Bridgford Foods Corp.'s Chicago plant as part of the Severe Violator Enforcement Program, which mandates follow-up inspections of employers that endanger workers through repeat violations, a release from the agency said. Bridgford was placed in the program following a July 2010 inspection for exposing workers to energized equipment and failing to implement and provide training on lockout and tagout procedures. Three repeat health violations involved failing to mark chemical containers with contents and hazardous warning labels and not providing an emergency eyewash station for employees working with corrosive chemicals such as sodium hypochlorite and anhydrous ammonia. Another repeat violation involved an obstructed emergency exit. Similar violations were cited in 2008 and 2010.
Source: http://www.suntimes.com/news/11603457-418/chicago-meat-processor-plant-draws-118700-osha-fines.html

27. *March 29, St. Marys Tribune & Georgian* – (Georgia) **State fines Kingsland Meats for violations.** A Georgia Department of Agriculture investigation cited Kingsland Meats in St. Marys, Georgia, for violating multiple rules in how it packages, labels, and processes its meat, the St. Marys Tribune & Georgian reported March 29. The department issued a stop-sale order to the store February 16 due to ground beef products not having the additive beef heart listed on the label. The order was lifted and the owner reopened Kingsland Meats March 1. Compliance specialists performed several inspections between October 2011 and March, after the department's meat inspection-compliance section received a complaint in October 2011 regarding Kingsland adding cardiac muscle to ground beef without listing the additive on labels. The order stated, "During the inspection on Feb. 15, numerous cases of beef hearts were observed in the freezer, which (the owner) stated he sold to a man for his dogs. During a detailed inspection on Feb. 16, 2012, (the owner) stated that he was adding beef hearts to his ground beef variety." Kingsland was applying Angus beef labels to meat products that were not Angus, and listing bull meat as ground round, the consent order said. It states an investigation by the department found numerous meat packages did not weigh the amount listed on the label. The investigation also cited Kingsland for improperly repackaging oysters and processing feral hogs without a license.
Source: http://www.tribune-georgian.com/articles/2012/03/30/news/top_stories/1topstory3.30.txt

For another story, see item **30**

[Return to top]

Water Sector

28. *March 29, KRMG 740 AM Tulsa* – (Oklahoma) **Water service restored to Okmulgee, 40,000 people.** A break at the water treatment plant west of Okmulgee, Oklahoma, was fixed and water service was restored, according to KRMG 740 AM Tulsa March 29. A new connection at the treatment plant broke March 28 and left 40,000 water customers in the area without water and under a boil order.

Source: http://www.krmg.com/news/news/local/water-service-restored-okmulgee-40000-people/nLf3J/

29. *March 29, Yakima Herald-Republic* – (Washington) **Wapato fined $57,000 for ammonia discharge.** Wapato, Washington, agreed to pay a fine of $57,000 for allowing its sewage treatment facility to discharge ammonia in violation of its Clean Water Act permit, the U.S. Environmental Protection Agency (EPA) announced March 29. The treatment facility exceeded permitted levels of ammonia more than 431 times between 2006 and 2010, according to the EPA news release, with ammonia constituting the majority of the problem discharges. The facility also discharged without a permit between June 2010 and September 2011. According to the city mayor, the wastewater treatment plant needs more than $7 million in upgrades to correct the ammonia discharge problem. Wapato has 4,605 residents.
Source: http://www.yakima-herald.com/stories/2012/03/29/wapato-fined-57-000-for-ammonia-discharge

30. *March 29, Hanover Evening Sun* – (Pennsylvania) **Thousands of gallons of milk spilled into Pa. stream.** A tanker truck overturned March 29 on state Route 94 just south of York Springs, Pennsylvania, spilling 4,000 gallons of milk into the stream that flows from the Huntington Township crash site to Lake Meade. State police said it would take several hours to clear the wreckage, and the stretch of road near the crash site could remain closed to traffic during much of that time. “It’s as bad as any HazMat spill,” the captain of the fire department said, explaining milk takes oxygen out of the water “and kills everything in it.” He said officials from the state department of environmental protection and the state department of transportation were at the scene. An area-wide response including emergency crews from as far away as Carlisle, Dillsburg, McSherrystown, and Gettysburg were called. Police said the driver of the milk truck was traveling south when the driver of a truck in front of him hit the brakes suddenly. The milk truck driver went off the side of the road and the truck overturned.
Source: http://www.firehouse.com/news/10685050/thousands-of-gallons-of-milk-spilled-into-pa-stream

31. *March 29, KAPP 35 Yakima* – (Washington) **Prosser water main breaks; spills one million gallons.** A water pipe in Prosser, Washington, burst March 29, sending about 1 million gallons of water rushing towards the highway, cemetery, and high school football field. According to a City of Prosser statement, the pipe burst for an unknown reason. Water rushed over Highway 22 from Paterson Road for a quarter of a mile down through the cemetery. Water was shut off to about 60 homes, but was fully restored by the afternoon. The water came from a 3-million gallon reservoir. An investigation is currently underway as to why the pipe burst, and examinations will be made to prevent future accidents.
Source: http://www.kapptv.com/article/2012/mar/29/prosser-water-main-breaks-spills-one-million-gallo/

32. *March 28, Associated Press* – (Missouri) **Cleanup plan formed for polluted Columbia creek.** The U.S. Environmental Protection Agency (EPA) and state department of natural resources unveiled a plan March 28 to reduce storm water runoff

in Hinkson Creek near Columbia, Missouri, found to be in violation of the federal Clean Water Act more than a decade ago. City government, Boone County, and the University of Missouri are also participating in the partnership, known as collaborative adaptive management. Hinkson Creek has been classified as an impaired waterway since 1998. A lawsuit filed against the EPA by the American Canoe Association and the Sierra Club led to a 2002 court order to bring the creek under federal clean water standards. The EPA established a total maximum daily load of allowed pollutants for Hinkson Creek in early 2011.
Source:
http://www.htrnews.com/usatoday/article/38911489?odyssey=mod|newswell|text|FRONTPAGE|s

For another story, see item **3**

[Return to top]

Public Health and Healthcare Sector

33. *March 30, YNN Central New York* – (New York) **Man arrested for bomb threat at hospital ER.** A New York Mills, New York man has been arrested for allegedly making a bomb threat in a Utica hospital emergency room, YNN Central New York reported March 30. Utica police say it happened at St. Elizabeth's Medical Center March 15. The man is accused of walking into the ER and saying he had a bomb in his car that he planned to detonate with his cell phone. Officers were able to take the cell phone from his shoe and located his car in the parking lot where they found a metal canister with a circuit board attached. A K-9 bomb detection team determined there was no threat. The man was arrested and charged with placing a false bomb, which is a felony.
Source: http://centralny.ynn.com/content/top_stories/578757/man-arrested-for-bomb-threat-at-hospital-er/

34. *March 30, Duluth News Tribune* – (Minnesota) **State cites Duluth methadone clinic for violations.** Duluth's only methadone clinic has fallen under tight scrutiny by the Minnesota Department of Health after the clinic was found to have 26 violations after an investigation fueled by complaints about the chemical-dependency treatment center. The clinic was cited for providing false information to investigators, inadequate oversight of patient medications, and sloppy paperwork on patients and staff. As of April 2, the Lake Superior Treatment Center's license will be on a "conditional" status from the state for 3 years. The clinic also was fined $400.
Source: http://www.duluthnewstribune.com/event/article/id/227124/

For another story, see item **46**

[Return to top]

Government Facilities Sector

35. *March 30, WYFF 4 Greenville* – (South Carolina) **Upstate schools affected by phone, Internet outage.** More than two dozen Greenville County Schools in South Carolina were experiencing phone and Internet outages March 30 due to an AT&T issue in the area. Greenville County schools officials said 28 schools were affected. Every school has an emergency communication system that allows administrators to remain in contact with the central office and call 911. AT&T said that significant damage occurred to a major AT&T fiber cable and there was no estimated time to repair.
Source: http://www.wyff4.com/r/30802700/detail.html

36. *March 29, Associated Press* – (California) **Security breach: Lost data cartridges may have exposed personal records from California's child support system.** Four computer storage devices containing personal information for about 800,000 adults and children in California's child support system – including their names and Social Security numbers – were lost by IBM and Iron Mountain Inc., officials announced March 29. There is a chance the information from the California Department of Child Support Services will not be accessible because a specialized machine is needed to run the cartridges the data is stored on, and special hardware and software are needed to read it, said a spokeswoman for the state's office of technology services. The cartridges also contained addresses, driver's license numbers, names of health insurance providers, and employers for custodial and non-custodial parents and their children. The department has notified all those possibly affected by the March 12 data loss via mail, and has notified the three major credit reporting agencies, the state attorney general's office and the state office of privacy protection.
Source: http://www.huffingtonpost.com/2012/03/30/lost-data-cartridges_n_1390258.html?

37. *March 29, Associated Press* – (Michigan) **Mich. militia head, son plead guilty to gun charge.** A Michigan militia leader and his son pleaded guilty March 29 to possessing a machine gun, giving prosecutors their only gain in a domestic terror trial that was upended when the judge dismissed charges of plotting war against the government. The leader and six militia members were cleared March 27 of conspiracy charges. Gun charges were all that remained for the leader and his son after the federal judge said prosecutors in 6 weeks had failed to present evidence of a specific plan to go to war against law enforcement and federal authorities.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5ieVw2p_yjO8H2uO6fGkMlHIhTOhQ?docId=cd331cd03992481d9027876b33a8cdda

38. *March 29, Softpedia* – (International) **MilitarySingles denies being hacked by LulzSec Reborn.** Recently, LulzSec Reborn claimed to breach MilitarySingles.com, leaking more than 170,000 record sets. At first the site's representatives said they were investigating the incident, now they came forward to deny the breach took place. DataBreaches obtained a second statement from ESingles, the company that manages MilitarySingles.com. "After a thorough investigation by our company programmers, it is our conclusion that our database was not hacked and that the claims of the Lulzsec

group are completely false," the organization's representative said. They reveal the number of records stored in their database does not even closely match the large number of records published online by the hackers, highlighting the fact that all the passwords are encrypted. Furthermore, they said the site was down March 25 for a scheduled maintenance and not because of a data breach. They also have an answer for the alleged defacement. According to the admin of MilitarySingles, the site was not defaced, instead an image was simply uploaded to their image repository.
Source: http://news.softpedia.com/news/MilitarySingles-Denies-Being-Hacked-by-LulzSec-Reborn-261591.shtml

39. *March 28, Nextgov* – (National) **Challenges remain in switch to govermentwide ID security system.** Federal agencies still are struggling to implement a government wide strategy for securing employee log-in credentials and smart card IDs, General Services Administration (GSA) representatives said March 28. Under a February 2011 directive from the Office of Management and Budget, all executive branches were supposed to have aligned themselves with Federal Identity, Credential, and Access Management (FICAM) by October 2011. FICAM standards are based on a former U.S. President-era Homeland Security Presidential Directive for streamlined and more secure verification procedures within the government. The director of GSA's identity assurance and trusted access division, noted March 28 at a conference at the International Spy Museum in Washington, D.C. that federal security has become so fragmented that some agencies are "almost issuing their own cards just for access to the cafeteria." The FICAM roadmap mandates that agencies switching to OpenID systems for easier Web site logins must "connect authoritative data sources and share data with the shared infrastructure." However, defining "authoritative" raises its own challenges, explained a GSA expert on digital security and service orientation. Though the federal government is not specifically required to use the OpenID blanket identification method for anything besides allowing citizens to logon to dot-gov Web sites, he said the system as it applies to mobile devices is a promising avenue for the government to explore.
Source: http://www.nextgov.com/nextgov/ng_20120328_8907.php

For more stories, see items **2**, **12**, **31**, and **46**

[Return to top]

Emergency Services Sector

40. *March 30, Associated Press* – (Colorado) **Colo. sheriff notes problems with fire warnings.** Colorado authorities said March 30 they were investigating problems with an emergency notification system because some residents who signed up never got a warning about a wildfire March 26. A Jefferson County sheriff's spokesman said that an unknown number of people who signed up were not called. The company that provides the system, FirstCall Network Inc., said everyone who signed up for the system did get a call. The company's president said the county can determine which phones, if any, were not called by comparing phone numbers in the system with mapping and telephone data. He said FirstCall was working with county officials.

Sheriff's officials said a couple found dead in the fire zone got a call, as did a woman who remains missing, but it was not immediately clear when the calls came. About 500 firefighters were working March 30 to contain more of the 6-square-mile wildfire, which was apparently sparked by a state controlled burn that sprang to life because of strong winds. It had damaged or destroyed at least 25 homes, and March 30, crews had cleared lines around 45 percent of its 8.5 mile perimeter. Residents of about 180 homes remained evacuated March 30. At the height of the fire threat, residents of about 900 homes were told to flee.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/03/30/national/a021524D56.DTL

41. *March 30, Softpedia* – (Nevada) **Las Vegas Police Department site breached by Pakistani hackers.** Pakistani hackers from the ZCompany Hacking Crew breached the recruitment Web site of the Las Vegas Police Department, Softpedia reported March 30. According to TechHerald, the hackers defaced the site and posted a message in which they accuse the United States of aiding Israel in maintaining a racist Jewish colony in Pakistan. ZCompany Hacking crew is one of the most vocal Pakistani hacker collectives, being involved in many hacktivist operations, such as Operation Free Palestine. In the past few months, they have defaced sites such as those of the Indian Highway Police, Fiat India, and thousands of commercial Web sites.
Source: http://news.softpedia.com/news/Las-Vegas-Police-Department-Site-Breached-by-Pakistani-Hackers-261793.shtml

For more stories, see items **2**, **19**, **37**, **48**, **50**, and **52**

[Return to top]

Information Technology Sector

42. *March 30, H Security* – (International) **Cisco patch day fixes nine IOS vulnerabilities.** As part of its bi-annual patch day, Cisco published nine security advisories for its IOS network operating system. These advisories address many vulnerabilities, one of which (CVSS 8.5) could allow unauthorized remote users to gain administrative access via a privilege escalation exploit. The other eight advisories cover denial-of-service (DoS) vulnerabilities. Several bugs in Cisco's IOS Zone-Based Firewall which left it vulnerable to DoS attacks. Other issues involve DoS problems when initiating NAT sessions, during Internet Key Exchange, establishing reverse SSH sessions, performing traffic optimization, handling multicast source discovery, or while using IOS's Smart Install feature.
Source: http://www.h-online.com/security/news/item/Cisco-patch-day-fixes-nine-IOS-vulnerabilities-1487219.html

43. *March 30, H Security* – (International) **Wireshark updates fix DoS vulnerabilities.** The Wireshark development team released versions 1.4.12 and 1.6.6 of its open source network protocol analyzer; these are maintenance updates that focus on fixing bugs and closing security holes found in the previous builds. The updates to the cross-platform tool address several vulnerabilities that could be exploited by an attacker

to cause a denial-of-service condition. These include a memory allocation flaw in the MP2T dissector that could cause it to allocate too much memory, a bug when trying to read ERF data using the pcap and pcap-ng file parsers, and a problem in the ANSI A dissector. To succeed, an attacker must inject a malformed packet onto the wire or convince a victim to read a malformed packet trace file. Versions 1.4.0 to 1.4.11 and 1.6.0 to 1.6.5 are affected; upgrading to the new releases corrects these problems. Another security bug affecting only the 1.6.x branch that could cause the IEEE 802.11 dissector to go into an infinite loop causing Wireshark to crash was also fixed.
Source: http://www.h-online.com/security/news/item/Wireshark-updates-fix-DoS-vulnerabilities-1487215.html

44. *March 30, CNET News* – (International) **Turning in an old Xbox? Consider hard drive data, report says.** Microsoft's Xbox 360 might not be protecting user data after the console is restored to factory settings, according to a new report. In an interview with gaming blog Kotaku, a researcher at Drexel University in Philadelphia said when Xbox 360 owners trade in their consoles after restoring the device to factory settings, their personal data might be left open to malicious hackers. "Microsoft does a great job of protecting their proprietary information," she told Kotaku. "But they don't do a great job of protecting the user's data." She, along with other researchers at the university, bought a refurbished Xbox 360 in 2011. Soon after, they downloaded some modding software, took aim at the device's hard drive, and eventually accessed the previous owner's credit card information.
Source: http://news.cnet.com/8301-13506_3-57407107-17/turning-in-an-old-xbox-consider-hard-drive-data-report-says/?part=rss&subj=news&tag=2547-1_3-0-20

45. *March 29, IDG News Service* – (International) **Do-it-yourself plan to take down Sality botnet outlined on public mailing list.** A method that anyone can use to hijack a massive multipurpose botnet called Sality was described in detail on a public mailing list March 27. Sality is a file-infecting virus that has been around for 9 years. More than 100,000 computers are infected with the malware and form a large peer-to-peer botnet used for various cybercriminal activities. An individual described how the Sality botnet can be destroyed or hijacked in an e-mail sent to the Full Disclosure mailing list. The e-mail's author linked to a Python script that can be used to determine update URLs queried by the botnet and said a Sality removal utility developed by antivirus firm AVG could be hosted on one of them to be downloaded and executed by the infected computers. Sality updates are usually hosted on compromised Web sites, so to replace them with the removal utility, someone would have to hack into those Web sites, like the Sality creators did, or persuade owners to willingly host the tool. There is a chance the plan may work, although the result would be unpredictable because each computer can have software and hardware particularities that come into play when the botnet is instructed to do something, said the principal manager at Symantec Security Response. Furthermore, forcing botnet clients to download and execute the removal tool is illegal because it involves modifying software on other people's computers without authorization. So the public availability of the takedown instructions is more likely to help cybercriminals who wish to hijack the botnet rather than legitimate researchers who want to disable it. Cybercriminals are probably already trying to use the information in the e-mail to their advantage, the Symantec researcher said. However,

Symantec has not seen any changes in the botnet since the takedown plan was posted online.
Source: http://www.computerworld.com/s/article/9225682/Do_it_yourself_plan_to_take_down_Sality_botnet_outlined_on_public_mailing_list?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Securit

46. *March 29, Dark Reading* – (International) **Bit9 sees a 150 percent increase in targeted domain controller attacks.** March 28, Bit9 announced it saw a 150 percent increase in the number of attacks on domain controllers year-over-year. Attackers, largely nation states and cyber criminals, are targeting intellectual property on these servers — everything from chemical formulas and vaccines to military data, and reports on global economic conditions. Rather than directly attacking servers that house the data, the attackers are specifically targeting domain controllers to gain access to all systems within the company. Because domain controllers store authentication data for everyone at an organization, they have become highly strategic targets for cyber criminals intent on stealing business critical data and conducting protracted attacks. In less than 15 minutes, cyber criminals can break in to domain controllers — also called Active Directory servers — to gain access to all user logins and passwords across an organization. While this information is typically encrypted, using new tools available on the Internet, often for free, cyber criminals can reverse engineer large stores of passwords and credentials within minutes.
Source: http://www.darkreading.com/advanced-threats/167901091/security/attacks-breaches/232700510/bit9-sees-a-150-percent-increase-in-targeted-domain-controller-attacks.html

47. *March 29, Softpedia* – (International) **Compromised OpenX ad servers lead users to malware.** Sophos researchers discovered a number of OpenX ad servers were compromised and altered to redirect users to sites that push dangerous pieces of malware. Experts found that when the OpenX ad content is requested by the browser, an iframe is also loaded, executing a malicious JavaScript identified as Troj/JSRedir-EF. The iframe added by the script loads content from a traffic directing server (TDS), controlled by a group called BlackAdvertsPro, which appears to be specializing in compromising Web sites to direct traffic to their own TDS. This traffic can be worth a lot of money if sold to criminals who run exploit sites. In one instance, the traffic was routed to an exploit site that served scareware called Smart Fortress 2012 (Mal/ExpJS-AF) by exploiting Java vulnerabilities. The BlackAdvertsPro crew seems to be checking IP addresses to ensure each visitor is directed only once to the exploit sites. “This supports the theory that they are selling the traffic to others running the exploit sites. (Attackers have no interest in paying for the same machine getting redirected to their exploit site multiple times.)” a principal virus researcher said. Ad content poisoning is a very popular technique among cybercriminals because it allows them to control large amounts of traffic. As many administrators and security enthusiasts are aware, traffic, especially high volumes, has high value on the underground markets.
Source: http://news.softpedia.com/news/Compromised-OpenX-Ad-Servers-Lead-Users-to-Malware-261713.shtml

For more stories, see items **35**, **36**, **38**, **39**, **41**, **48**, and **50**

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

48. *March 30, Associated Press* – (Ohio) **Southern Ohio loses 9-1-1, ATM, data service when thief steals fiber-optic cable.** Scrap metal thieves targeting fiber optic cables shut down 9-1-1 service in Ohio's Appalachian region and left thousands without telephone and Internet services. WBNS 10 Columbus reported four counties in southern Ohio were affected by the outage, which started late March 28 and lasted until the afternoon of March 29. Frontier Communications said fiber optic cables were cut and stolen, affecting 8,000 customers in Pike, Scioto, Jackson, and Lawrence counties at Ohio's southern tip. Credit card readers and ATMs also were affected. Frontier Communications said state police are investigating.
Source: http://www.cleveland.com/metro/index.ssf/2012/03/southern_ohio_loses_9-1-1_atm.html

49. *March 30, Aurora Beacon-News* – (Illinois) **Copper stolen from 3 Verizon cell towers.** Large amounts of copper was stolen from three communication towers throughout Kendall County, Illinois, in March, according to reports March 29 from the Kendall County Sheriff's Department and Oswego Police. Copper valued at $1,000 was stolen between March 3 and March 28 from a communications tower in Oswego, police said. Two other incidents occurred between March 15 and March 29. Silver-colored copper "busbars" valued at $4,000 were stolen from a communications tower and similar copper pieces, valued at $8,000, were stolen from a tower in Yorkville, the sheriff's office said. All three towers are owned by Verizon Wireless.
Source: http://beaconnews.suntimes.com/news/11604035-418/copper-stolen-from-3-verizon-cell-towers.html

50. *March 29, KOKI 23 Tulsa* – (Oklahoma) **AT&T service restored in Mayes County.** An AT&T fiber optic cable was cut in Mayes County, Oklahoma, March 29 forcing almost 50,000 people in Green County to communicate without cell phones or the Internet. AT&T crews said a man was burying his trash off Highway 20 and 427 Road when his tractor cut through the fiber optic cable. The Mayes County 911 center had to route their calls through to Rogers County's 800 radio system, and then send them back to Mayes County dispatchers. By 8 p.m., crews had finished repairing the fiber optic line.
Source: http://www.fox23.com/news/local/story/AT-T-service-restored-in-Mayes-County/WsF8o6-gs02ouIkgpA-_wg.cspx

For another story, see item **35**

[Return to top]

Commercial Facilities Sector

51. *March 29, KSL-TV 5 Salt Lake City* – (Utah) **Cigarette causes early morning fire, displaces 120.** More than 100 tenants of a Salt Lake City apartment complex were forced from their homes because of a two-alarm fire March 29. About 30 people had to be rescued from their balconies with ladders. The fire broke out after a tenant fell asleep on a recliner while smoking. The apartment where the fire started suffered heavy fire damage. Fifteen other units suffered smoke or water damage. Total damage was estimated at $150,000. A fire department spokesman estimated about half of those tenants would be back in their apartments by March 29. The other half would probably be out of their homes a few days.
Source: http://www.ksl.com/?nid=148&sid=19777840&title=early-morning-fire-displaces-75&s_cid=featured-1

52. *March 29, WEWS 5 Cleveland* – (Ohio) **Fire extinguished after gas line rupture near Lyndhurst apartment building.** More than 100 firefighters battled a large fire after construction crews ruptured a gas line next to an apartment building in Lyndhurst, Ohio, March 29. Emergency crews responded as soon as they learned of the 4-inch gas line rupture, and evacuated all the residents from the building. A short time later, the gas caught fire and crews struggled to turn off the pipeline feeding the main. The fire department said the gas spread through the first, second, and third floors, with most of the damage confined to one wing of the building. The gas line was shut off and the fire was put out after about 3 hours. Three firefighters were accessed on the scene for injuries and one resident was taken to a hospital. Residents were allowed to return to their units for essential items March 30. The fire department was not sure when residents would be permitted to return permanently.
Source: http://www.newsnet5.com/dpp/news/local_news/oh_cuyahoga/firefighters-battling-fire-gas-leak-at-lyndhurst-apartment-building

For more stories, see items **31**, **40**, and **55**

[Return to top]

National Monuments and Icons Sector

53. *March 30, TriCities.com* – (Virginia) **Firefighters battling Smyth County wildfire.** A 100-plus acre wildfire burned late into the night March 29 in Smyth County, Virginia. Some summer homes were threatened by the blaze early on, a Saltville Volunteer Fire Department assistant chief said March 29. But by evening, the fire had moved beyond the homes in Saltville. Firefighters initially suspect “something happened to the power line” and one fell, sparking the fire. The fire is one of four large wildfires reported in the area during 2012 –- two have burned a combined 1,000 acres in the Blackwater section of Lee County, Virginia, and one burned more than 100 acres in Coeburn,

Virginia. Virginia is currently under a burning ban –- fires are permitted only between the hours of 4 p.m. and midnight. The ban is in effect during fire season, from February 15 to April 30.
Source: http://www2.tricities.com/news/2012/mar/30/firefighters-battling-smyth-county-wildfire-ar-1805054/

For another story, see item **40**

[Return to top]

Dams Sector

54. *March 30, Yankton Daily Press & Dakotan* – (South Dakota) **Corps to inspect spillway area.** To survey possible damage caused by high releases during 2011's summer flooding, the U.S. Army Corps of Engineers will begin an underwater inspection March 30 of the spillway apron at Gavins Point Dam near Yankton, South Dakota. The Corps has been inspecting parts of the spillway not under water, and contracted divers will move forward with an extensive inspection of the spillway apron. The project operations manager said the main focus of the inspection will be on the condition of about 250 drains that help release hydraulic pressure in the spillway. The inspection will also include ground penetrating radar to determine the condition of the concrete slab and the gravel frost blanket underneath the concrete. The inspection is expected to be complete April 6. Boating and fishing will be prohibited in the spillway area during the inspection.
Source: http://www.yankton.net/articles/2012/03/30/community/doc4f752e6c489e4004411453.txt

55. *March 29, New Orleans Times-Picayune* – (Louisiana) **National Guard to close parts of Bonnet Carre Spillway Saturday for drill.** The Louisiana National Guard and several other state agencies planned to conduct a disaster-response exercise in the Bonnet Carre Spillway in St. Charles Parish March 31, closing portions of the recreation area to the public. According to the U.S. Army Corps of Engineers, it will be the first exercise in 3 years to be held at the spillway. The exercise will allow the state to prepare for any potential hurricanes or other emergencies with mock search-and-rescue operations, emergency infrastructure repair and construction exercises, and sandbag-placement operations. The public will be allowed to view the exercise from a designated area near eastbound Airline Drive.
Source: http://www.nola.com/politics/index.ssf/2012/03/national_guard_to_close_parts.html

[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