Daily Open Source Infrastructure Report
30 April 2012

Top Stories

- A court required a man and his companies to pay a $5 million penalty for running a foreign currency scam that cheated at least 500 investors out of $85 million. – *U.S. Commodity Futures Trading Commission* (See item **10**)
- Forty more illnesses were added to the multi-state outbreak linked to Salmonella-contaminated sushi tuna, bringing the total cases to 200 in 26 states. – *Food Safety News* (See item **18**)
- A hacker who released source code from hypervisor VMware, a platform that runs guest operating systems for many businesses and organizations, threatened to release more data May 5. The source code could allow malicious actors to take advantages of vulnerabilities in such systems. – *InformationWeek* (See item **36**)
- A researcher said a remotely exploitable vulnerability exists in all current versions of the Oracle database server. It allows an attacker to intercept traffic and execute arbitrary commands on the server. – *Threatpost* (See item **37**)

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 27, Associated Press* – (Texas) **7 workers in Brownsville sick from carbon dioxide.** Emergency officials said seven workers at an oil and gas maritime services company in Brownsville, Texas, were overcome by leaking gas April 26. The Brownsville Fire Department chief said the men became ill following a carbon dioxide leak. The chief said all seven workers were in stable condition when they were transported to a hospital. Company officials said the men are employed by a contractor and were working on a fire suppression system on a vessel. Keppel AmFELS builds and services mobile drilling rigs and platforms.
Source: http://abclocal.go.com/ktrk/story?section=news/state&id=8638495

2. *April 26, Associated Press* – (Wyoming) **Wind shift delays efforts to plug blown Wyo. well.** A wind shift was holding up attempts to plug an oil well spewing methane gas after a blowout in east-central Wyoming, the Associated Press reported April 26. Workers with Houston-based well control company Boots & Coots were not able to safely get close enough to the well by late April 26. The blowout happened April 24. The risk of an explosion and fire continued as did a voluntary evacuation order that applied to 67 residents within 2.5 miles of the well, according to the Converse County emergency management coordinator. About 50 people heeded the evacuation advisory but were being allowed to come and go to check on their property. The blowout happened as workers were installing steel casing down the well, which had been drilled to nearly 18,000 feet horizontally and vertically. The well was targeting the Niobrara Shale formation that underlies eastern Wyoming, northern Colorado, and western Nebraska.
Source: http://www.summitdaily.com/article/20120426/NEWS/120429838/1078&ParentProfile=1055

3. *April 26, Charleston State Journal* – (National) **MSHA to phase out potentially faulty breathing devices.** Federal mine safety officials have ordered immediate phase-out of a self-contained self-rescue device (SCSR) found to have potential for failure, the Charleston State Journal reported April 26. The breathing devices were found to have a "low-probability" of failure, so the agency ordered the SCSR devices from Pittsburgh-based CSE corp. to be removed from the nation's mines. The Mine Safety and Health Administration (MSHA) made the announcement April 26. "Due to the large number of CSE SR-100s in underground coal mines, multiple SCSRs available to miners, the low probability of failure and the shortage of immediately available replacements, MSHA and [the National Institute for Occupational Safety and Health (NIOSH)] have determined an orderly phase-out will better protect the safety of miners than immediate withdrawal of the devices," said the assistant secretary of labor for mine safety and health. The rescue devices are designed to provide underground coal miners with up to

60 minutes of breathable air in the event of an emergency. A joint investigation by the NIOSH and the MSHA found the units did not conform to safety requirements. Source: http://www.statejournal.com/story/17795242/msha-to-phase-out-potentially-faulty-breathing-devices

[Return to top]

Chemical Industry Sector

4. *April 27, Cleveland Sun News* – (Ohio) **Fire hits Avon's Chemtron Corp. in the early morning hours.** Avon, Ohio firefighters responded to a fire at the Chemtron Corporation facility early April 27. The Avon fire chief said they found materials on a pallet on fire. Officials said there was a lot of smoke so it took about an hour to ventilate the building. They said preliminary findings indicate the fire was probably caused by some type of chemical reaction. Fire damage was mainly isolated to the products on the pallet and a tow motor with some smoke damage to the ceiling. Source: http://www.cleveland.com/avon/index.ssf/2012/04/fire_at_avons_chemtron_corp_in.html

5. *April 26, Mobile Press-Register* – (Alabama) **Olin plant in McIntosh partially closed due to chlorine leak.** A chlorine leak April 25 at the Olin Corp. plant in McIntosh, Alabama, forced a shutdown of part of the facility, which manufactures chlorine, for a few days. Company officials described the leak as small and said a monitoring system detected the release of the deadly gas. The leak, which a federal incident report stated was caused by "equipment failure," was isolated. Production was stopped in the affected section of the plant April 25 and April 26, and was to remain stopped while the company investigates the leak. In a statement, Olin officials wrote that neither employees nor people living in the community surrounding the plant were in danger. Source: http://blog.al.com/live/2012/04/olin_plant_in_mcintosh_partial.html

For more stories, see items **13**, **21**, and **26**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

Nothing to report

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

6. *April 26, Global Security Newswire* – (National) **Miscoordination slows U.S. missile defense preparations: GAO.** The U.S. Defense Department's strategy of simultaneously pursuing multiple preparatory phases for its missile defense systems has resulted in unnecessary delays of certain equipment, the Government Accountability Office (GAO) said in a report issued April 25. Drawing from previous GAO findings, congressional auditors found such parallel operations to exist at "high levels" in policies the Pentagon's Missile Defense Agency adopted previously and in the present to obtain antimissile systems. The antimissile office has pursued many reforms, but "considerable risk" would persist for "future performance shortfalls that will require retrofits, cost overruns, and schedule delays" if the Pentagon pursues such simultaneous preparations for antimissile efforts at later dates, the report warns. The Pentagon endorsed six of seven guidelines provided by Congressional investigators for curbing such practices and "partially agreed" with the remaining advisory statement. Separately, the Missile Defense Agency is taking many steps in response to concerns voiced by GAO auditors in June 2011 over possible problems with antimissile components, the document states. The measures involved "internal policies, collaborative initiatives with other agencies, and contracting strategies to hold its contractors more accountable," investigators wrote.
   Source: http://www.nti.org/gsn/article/miscoordination-slows-us-antimissile-preparations-gao/

For more stories, see items **31** and **36**

[Return to top]

Banking and Finance Sector

7. *April 27, Philadelphia Inquirer* – (Pennsylvania; New Jersey) **Glenside broker among six charged in loan-fraud case.** Federal prosecutors in Philadelphia indicted a business-loan broker and his business partner April 26 on charges of fraud, conspiracy, and money-laundering, alleging the pair "defrauded more than 800 victims out of more than $10 million," according to a statement from a U.S. attorney, FBI special agent-in-charge, and a U.S. Internal Revenue Service acting special agent-in-charge. The defendant is the founder and chairman of Philadelphia-based Remington Capital Group and related companies. Also charged with fraud were four brokers. According to the indictment, between 2005 and 2011 the two men and their brokers "fraudulently induced hundreds of people to pay Remington fees in excess of $10,000 apiece, based on false representations that Remington had lenders and/or investors ready to provide financing for the victims' projects." Victims included a New Jersey developer trying to raise $27.5 million for a Camden project and a Pennsylvania developer trying to raise $22 million for a solar electric farm, the indictment said. In many cases, according to the indictment, the suspect never had funding lined up but "fraudulently" took fees anyway.
   Source: http://www.philly.com/philly/business/149140135.html

8. *April 26, Minneapolis Star Tribune* – (Minnesota) **Ex-Centennial Mortgage executive pleads guilty to bank fraud.** A former executive with Centennial Mortgage and Funding Inc. pleaded guilty April 26 in a Minneapolis federal court to defrauding various banks to cover the company's losses and fund its operations. The executive was an accountant, senior vice president, and chief financial officer for the mortgage company in 2007 and 2008, when the alleged fraud took place. The government contended he was responsible for $8 million in losses. Centennial, a mortgage lender, had warehouse lines of credit with various banks, including American Bank. The executive admitted misleading lenders about the status of existing mortgage loans to get them to advance Centennial more money; helping conceal defaults on existing mortgage loans; hiding the fact that about 23 mortgage loans were double-funded; and kiting checks between Centennial's various bank accounts. He used the money he obtained for payroll and other operating expenses, the government said. He said he did not do all those things personally, but he failed to inform the financial institutions about what he knew and aided others in the alleged fraud.
   Source: http://www.loansafe.org/ex-centennial-mortgage-executive-pleads-guilty-to-bank-fraud-2

9. *April 26, Seattle Times* – (Washington) **Columbia City bank damaged by Molotov cocktail.** A bank in the Columbia City section of Seattle damaged overnight April 26 when someone threw a Molotov cocktail at the side of the building, according to Seattle police. When employees arrived April 26, they discovered a broken window and burn marks on the side of the building. A police account of the incident said it appeared the gasoline-filled bottle struck and scorched the side of the bank. It did not cause significant damage.
   Source: http://blogs.seattletimes.com/today/2012/04/columbia-city-bank-damaged-by-molotov-cocktail/

10. *April 26, U.S. Commodity Futures Trading Commission* – (California; National) **Federal court enters order settling CFTC $85 million forex fraud action against a California resident and his companies SNC Asset Management, Inc. and SNC Investments, Inc.** The U.S. Commodity Futures Trading Commission (CFTC) obtained a federal court supplemental consent order requiring a defendant and his companies, SNC Asset Management, Inc., and SNC Investments, Inc., to pay a $5 million civil monetary penalty, the CFTC announced April 26. The court's supplemental consent order, filed in California, resolves a CFTC complaint that charged the defendants with operating an $85 million fraudulent foreign currency (forex) scam. According to the consent order, the defendants fraudulently solicited at least $85 million from at least 500 customers to trade forex. The defendants in their solicitations falsely claimed to be operating successful forex trading firms and guaranteed monthly returns generated by their trading, the order finds. These representations, and subsequent fictitious account statements depicting profitable returns on individual accounts, created the false impression the defendants were trading forex profitably, the order finds. However, only a small percentage of the $85 million solicited was traded and the defendants' limited trading resulted in losses, according to the order. Rather than trade on behalf of customers, the defendants misappropriated customer funds for personal use. In a related criminal action, the defendant pleaded

guilty April 9, 2010 to conspiracy to commit wire fraud and conspiracy to commit money laundering.
Source: http://www.cftc.gov/PressRoom/PressReleases/pr6245-12

11. *April 26, Fox Business Network* – (New York; National) **NYSE receives credible cyber threat against website.** The New York Stock Exchange (NYSE) received a credible threat to disrupt its external Web site as part of an apparent cyber attack attempt against many U.S. exchanges, the Fox Business Network reported April 26. The threat, which is not tied to NYSE's trading systems, prompted the Big Board to beef up security and monitoring for a potential cyber attack, sources familiar with the matter said. The April 26 threats centered around a potential denial-of-service attack strictly focused on the exchange's external Web site, and having nothing to with its trading systems, a source said. The cyber threat appears to be tied to an anti-capitalistic online posting by a cyber group called "L0NGwave99" that promised to hit stock exchanges with a denial of service attack April 26 in support of the "great and rooted 99% movement." In addition to the NYSE, the group claimed it will put "into a profound sleep" the Web sites of the Nasdaq Stock Exchange, BATS, the Chicago Board of Options Exchange, and the Miami Stock Exchange. While the posting said it would start the operation at 9 a.m., none of those exchanges appeared to be suffering any Web site difficulties as of early the afternoon of April 26.
Source: http://www.foxbusiness.com/industries/2012/04/26/nyse-receives-credible-cyber-threat/

[Return to top]

Transportation Sector

12. *April 27, KARE 11 Minneapolis* – (Minnesota) **Humphrey terminal reopened after suspicious package scare.** The Hubert H. Humphrey terminal at the Minneapolis-St. Paul International Airport was cleared and reopened after a suspicious bag was found during pre-screening early April 27. A Metropolitan Airports Commission spokesperson said the suspicious bag set off an alarm during security pre-screening. Airport security could not resolve the situation so a decision was made to call in the Bloomington Police Bomb Squad. Passengers who were already inside the pre-screening area were allowed to stay in the terminal, but anyone that arrived after the discovery of the package was diverted to the parking ramp across the street from the Humphrey terminal. Almost 2 hours later, the bomb squad secured the bag and removed it from the terminal. The owner of the suspicious bag was detained for questioning. Metro Transit reported the activity did not affect light rail service to the airport.
Source: http://www.kare11.com/news/article/974617/391/Humphrey-terminal-reopened-after-suspicious-package-scare?odyssey=tab|topnews|bc|large

13. *April 27, Fort Worth Star-Telegram* – (Texas) **Tanker truck wreck and fire close I-35W in Alvarado.** A wreck on Interstate 35W near Alvarado, Texas, resulted in a tanker trunk fire that forced the closure of the highway in both directions, backing up traffic for miles April 27. Fire crews extinguished the fire and hoped to soon open the

northbound service road, said a spokesman for the Texas Department of Transportation. The main northbound Interstate 35W lanes however, were expected to be closed for much of the day. The southbound lanes have reopened, the spokesman said. The wreck involved the tanker hauling the gasoline-additive methanol, and an 18-wheeler and occurred near the interstate's intersection with U.S. 67, he said.
Source: http://www.star-telegram.com/2012/04/27/3917142/tanker-truck-wreck-and-fire-close.html

14. *April 27, WSYR 9 Syracuse* – (New York) **I-81 Northbound still closed in Cortland County.** I-81 Northbound remained closed April 27 after a bridge was struck the prior evening in Cortland County, New York. Emergency dispatchers said a truck towing heavy equipment on Preble Road struck the bridge. As a result, dispatchers said the New York State Department of Transportation closed a portion of the northbound lanes so crews could inspect and assess any damage to the bridge. State police said the roadway would remain closed for an "unknown duration."
Source: http://www.9wsyr.com/mostpopular/story/I-81-Northbound-still-closed-in-Cortland-County/ph1WmdsW2kGLRgM_PT088w.cspx

15. *April 26, KTRK 13 Houston* – (Texas) **Four shots fired at HISD bus with kids on board.** A recently released video shows what happened inside a Houston Independent School District bus full of students in Houston when someone started shooting at it March 27. The bus left Beechnut Academy with about 26 students on board, KTRK 13 Houston reported April 26. District police said some students on the bus flashed gang signs at someone walking on the street. That person then pulled a gun and fired at the bus on the Southwest Freeway Feeder. Investigators sought public help in identifying the shooter. A bullet struck near one of the windows on the bus, injuring one student.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=8637921

16. *April 26, Lakeland Ledger* – (Florida) **Polk school bus collision on S.R. 60 sends eleven students to hospital.** A car rear-ended a Polk County, Florida school bus on State Road 60 near Bartow, April 26, sending 11 students and 2 bus workers to the hospital. The crash happened as the bus, which held about 31 children from Bartow Middle School, headed east on S.R. 60, authorities said. It slowed to make a right turn then drop off students. A car driver struck the left rear of the bus, authorities said. The car spun counter-clockwise and came to rest in the eastbound lanes of S.R. 60. Some on the bus had minor injuries, while others were taken to hospitals for observation purposes only. The students who were not injured were taken home by another bus.
Source:
http://www.theledger.com/article/20120426/NEWS/120429463/1134?Title=Polk-School-Bus-Collision-on-S-R-60-Sends-Eleven-Students-to-Hospital

17. *April 26, WBBM 2 Chicago* – (Illinois) **Crews quarantine Delta airliner at Midway– for passenger with bug bites.** A suspected medical problem with a passenger on Delta Airlines flight 3163 from Detroit led emergency crews to quarantine the plane at Midway Airport in Chicago April 26. Chicago fire department crews surrounded the Delta airliner near Gate A7 at the airport. Passengers were allowed off the plane after about 2 hours on the tarmac. The passenger who sparked fears about a potentially

contagious disease visited Africa before changing planes in Detroit. It turned out to be a false alarm. Health officials determined the rash was probably bed-bug bites.
Source: http://chicago.cbslocal.com/2012/04/26/fire-crews-surround-delta-airliner-at-midway-for-medical-emergency/

For another story, see item **42**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

18. *April 27, Food Safety News* – (National) **Multistate outbreak linked to raw sushi grows to 200 cases.** Forty more illnesses were added to the multi-state outbreak linked to Salmonella-contaminated sushi tuna, the Centers for Disease Control and Prevention (CDC) reported April 26. The CDC also announced that health officials grouped a second strain of Salmonella Nchanga into the outbreak investigation. As of late the week of April 23, the CDC said there were 160 confirmed cases of Salmonella Bareilly linked to the same outbreak. Now, it is reporting 190 illnesses in 21 states linked to Salmonella Bareilly, and 10 illnesses in 5 states linked to Salmonella Nchanga. The product implicated, known as "tuna scrape," is raw yellowfin tuna that has been shaved and recovered from tuna bones, which is served raw in sushi products, particularly spicy tuna rolls. The Nacaochi Scrape fish product was imported from India and has been recalled by the California-based distributor, Moon Marine USA. At least two more people were hospitalized since the CDC's last update, bringing the total to 28. New York reported the most cases, with 35 sickened. Massachusetts had 24 cases. Maryland had 20 cases, while New Jersey had 19. Wisconsin reported 16, Illinois 15, Georgia 11, and Virginia 10. Connecticut had eight cases, followed by Pennsylvania with seven, and Rhode Island with six. Texas and Missouri were reporting four cases. South Carolina, North Carolina, and Louisiana each reported three. Alabama, Mississippi, and Washington, D.C. each had two. Arkansas and Florida reported one case.
Source: http://www.foodsafetynews.com/2012/04/multistate-outbreak-linked-to-raw-sushi-grows-to-200-cases/

19. *April 27, Food Safety News* – (New York) **Sprouts recalled due to Listeria risk.** About 100 pounds of Springwater Sprouts brand Organic Alfalfa Sprouts and 3# Bulk Clover Sprouts were recalled because of possible contamination of Listeria monocytogenes, Food Safety News reported April 27. The sprouts, distributed by Alfa Sprouts Inc. of Honeoye Falls, New York, come in two packages: clear clam shell packages containing 4-ounce Organic Alfalfa Sprouts that were distributed in New York State and 3# bulk containers of Clover Sprouts that were distributed to

institutional accounts in Upstate New York. The Listeria contamination was discovered after sampling by New York State Department of Agriculture inspectors and analysis by the New York State Food Laboratory.
Source: http://www.foodsafetynews.com/2012/04/alfalfa-sprouts-recalled-due-to-listeria-risk/

20. *April 27, Food Safety News* – (National) **Allergen alert: Mispackaged hostess candy mix.** Krispak of Grand Rapids, Michigan, recalled 16 cases of GFS Hostess Candy Mix in 8- to 48-ounce packages due to a packaging error, Food Safety News reported April 27. A small number of cases of the Hostess Candy Mix were inadvertently put into GFS Chocolate Sprinkles packages. The Hostess Candy Mix contains wheat and milk and may contain egg, none of which are declared on the Chocolate Sprinkles package. The recalled Hostess Candy Mix was distributed from April 5 through April 19 to Indiana, Ohio, Michigan, Kentucky, Pennsylvania, and Tennessee Gordon Food Service Marketplace Stores.
Source: http://www.foodsafetynews.com/2012/04/allergen-alert-mispackaged-hostess-candy-mix/

21. *April 27, Twin Falls Times-News* – (Idaho) **EPA fines Idaho milk products $52,000.** A Jerome, Idaho dairy processing facility will pay close to $52,000 in fines for failing to report its prior use of toxic chemicals. The U.S. Environmental Protection Agency announced April 26 that Idaho Milk Products did not disclose its use of nitric acid in 2009 on time. Nitric acid is one of the toxic chemicals that must be disclosed under the agency's right-to-know laws called the Toxics Release Inventory Program. According to court documents, Idaho Milk Products used 300,000 pounds of nitric acid and manufactured more than 25,000 pounds of nitric compounds in 2009. The company eventually filed the appropriate documents for using the chemical but did so 360 days late. The failure to disclose was a result of an "oversight," according to an Idaho Milk Products statement. The facility has corrected the situation by improving its reporting process and creating a new position designed to oversee environmental compliance, according to its statement.
Source: http://magicvalley.com/business/local/epa-fines-idaho-milk-products/article_6c2d72dc-9d9b-5c04-9b1f-615d7fb5c625.html

22. *April 27, Omaha World-Herald* – (Nebraska) **E. coli discovery idles meat plant.** The discovery of E. coli in beef produced April 25 at the JBS meatpacking plant in Grand Island, Nebraska, caused the plant to cease full production until April 27. Trim meat tests found that some of the cattle brought into the plant had E. coli and that E. coli had gotten onto produced meat cuts. Although the plant has a tracking system to indicate exactly which cuts of meat and carcasses tested positive for E. coli, the policy is to clean and retreat all the meat processed within a half-day of the positive test, a JBS spokesman said. Employees cleaned the plant, but slaughter ceased and incoming cattle trucks were turned back, he said. There are no recalls of any product associated with the E. coli discovery, as it was found before any product went to market.
Source: http://www.omaha.com/article/20120427/NEWS01/704279898/-1

23. *April 26, Food Safety News* – (National) **Improperly eviscerated vobla fish recalled.** LA Star Seafood Co. of Los Angeles recalled fish products labeled as Vobla Dry and Vobla Smoked because they were improperly eviscerated and have the potential to be contaminated with Clostridium botulinum, Food Safety News reported April 26. Consumers were warned not to use the product even if it does not look or smell spoiled. The U.S. Food and Drug Administration discovered the problem during an inspection. The sale of improperly eviscerated fish, 5 inches in length or greater, is prohibited because Clostridium botulinum spores are more likely to be concentrated in the viscera than any other portion of the fish. Uneviscerated fish has been linked to outbreaks of botulism poisoning which may pose a potentially life-threatening health hazard. Products were distributed and sold at: Arbat Store in Utah; European Importing, Russian Import, and M and M Market in northern California; Golden Farms Market, Karabagh Market, and Tashkent Market in southern California; Global Importing in Oregon; and Solomon's Groceries and Europa in Colorado.
Source: http://www.foodsafetynews.com/2012/04/improperly-eviscerated-vobla-fish-recalled/

24. *April 26, Food Safety News* – (Missouri) **Raw milk dairy named as possible source in Missouri E. coli outbreak.** The Missouri Department of Health and Senior Services April 25 named Stroupe Farm in Howard County as the possible source of an ongoing E. coli O157:H7 outbreak in central Missouri. The health department also narrowed their outbreak investigation from 15 cases down to 12, removing the 3 cases that did not share similar lab results, geographic proximity, or case history. Eight of the 12 individuals reported consuming raw milk or raw milk products from Stroupe Farm. Of the other four, two were related to people who consumed raw milk, while the remaining two had infections that genetically matched the others despite the individuals reporting no connection to raw dairy. Early in the investigation, the Missouri State Public Health Laboratory analyzed eight samples of products from the farm, all of which tested negative for E. coli O157:H7. Regardless, the owner of the farm discontinued the sale of raw dairy products, according to a state health department spokeswoman. A toddler who consumed raw milk products was hospitalized for more than 2 weeks after developing symptoms of hemolytic uremic syndrome, a kidney disease associated with severe E. coli infections.
Source: http://www.foodsafetynews.com/2012/04/raw-milk-dairy-named-as-possible-source-in-missouri-e-coli-outbreak/

[Return to top]

Water Sector

25. *April 27, Hazleton Standard Speaker* – (Pennsylvania) **1.8 million gallons of sewage leaks into river in Tamaqua.** Contractors in Tamaqua, Pennsylvania, finished patching a concrete pipe April 26 through which workers accidentally drilled while sinking a caisson for a temporary bridge, causing up to 1.8 million gallons of sewage to spill into the Little Schuylkill River, April 25. The State Department of Environmental Protection planned to continue to investigate how the accident occurred and whether any penalties will be assessed, the department's spokeswoman said. She noted that the

section of the river near the bridge is tainted by acid water from mine workings. Tamaqua wastewater treatment plant officials noticed flow in the plant plummeted from 1,700,000 gallons a day to 200,000 gallons per day, leading to the discovery of the broken pipe. Workers built a coffer dam to keep river water away from the sewage outfall and rigged pumps to push the sewage to a manhole downstream.
Source: http://republicanherald.com/news/1-8-million-gallons-of-sewage-leaks-into-river-in-tamaqua-1.1306715

26. *April 26, Athens News Courier* – (Alabama) **State files suit against Ardmore water and sewer.** Citing violations of the Alabama Water Pollution Control Act, the Alabama attorney general filed a lawsuit against Ardmore's Water Works and Sewer Board April 11, the Athens New Courier reported April 26. The suit alleges that Ardmore's wastewater treatment facility discharges pollutants into Piney Creek, a tributary of the Tennessee River, and seeks to recover $25,000 per violation. A similar suit was filed by Tennessee Riverkeeper officials who discovered an alleged 2,024 violations of the Clean Water Act, and that the Ardmore Water Board exceeded discharge limitations for ammonia, biochemical oxygen demand, E. coli, and other suspended solids. The alleged violations occurred from August 2007 to the present.
Source: http://enewscourier.com/local/x296818977/State-files-suit-against-Ardmore-water-and-sewer

27. *April 26, Associated Press* – (Indiana) **8-mile tunnel planned for Indianapolis sewage.** Work is starting on an 8-mile-long tunnel under the south side of Indianapolis that is the first major part of a $1.6 billion project aimed at reducing the release of raw sewage into the city's rivers, officials announced April 26. The plan calls for crews to bore the 18-foot diameter tunnel about 250 feet underground between a sewage treatment plant on the city's far south side to a location near the White River. The work is expected to take 5 years and be followed by 4 shorter tunnels that will contain water after storms from the city's combined storm and sanitary sewers until it can be treated. The project is required under a 2006 agreement between the city and federal and state environmental agencies to reduce sewage releases into waterways by 2025. When complete, city officials said the 25 miles of tunnels will be able to store 250 million gallons during and after rainstorms, and reduce untreated sewage overflow by at least 95 percent. Money for the project is coming from recent annual hikes in city sewer rates, including a 10.8 percent increase in 2012, and a similar increase planned for 2013.
Source:
http://www.wisconsinrapidstribune.com/usatoday/article/39141657?odyssey=mod|newswell|text|FRONTPAGE|s

[Return to top]

Public Health and Healthcare Sector

28. *April 27, Nashville Tennessean* – (Tennessee) **Tick-borne Rocky Mountain spotted fever cases jump in TN.** Cases of tick-borne Rocky Mountain spotted fever are up 533 percent the spring of 2012 compared to the same period in 2011, the Tennessee

Department of Health said April 26. The state agency is advising people to take extra precautions when outdoors. A mild winter and a warmer-than-normal March brought out ticks earlier in 2011. Rocky Mountain spotted fever can be a severe or even fatal illness if not treated in the first few days of symptoms, according to the Centers for Disease Control. Parents are urged to check children for ticks after they have played outdoors. Repellents containing DEET can be applied to skin, while those containing permethrin can be sprayed on shoes and clothing. People are urged to check thoroughly for ticks when they have been in grass or wooded areas.
Source: http://www.wbir.com/health/article/218080/3/Tick-borne-Rocky-Mountain-spotted-fever-cases-jump-in-TN

[Return to top]

Government Facilities Sector

29. *April 27, Somerville Courier News; East Brunswick Home News Tribune* – (New Jersey) **6th bomb threat at Union County College evacuates Cranford campus.** The Union County College campus in Cranford, New Jersey, was evacuated April 27 after the school received its sixth threat in the same month. The county's bomb squad searched the buildings and the Cranford police issued an "all clear" about 30 minutes after buildings were evacuated, the school vice president said. The "threatening call" was the fifth such call to the Cranford campus in April. The school's Plainfield campus received a bomb threat April 20. The last threat the school received was April 24, which the school vice president described as "very vague." That call did not result in an evacuation. All of the threats in April turned out not to be credible, although they caused disruptions for students, employees, and law enforcement. The false alarms are under investigation by the FBI, officials said.
Source:
http://www.mycentraljersey.com/article/20120427/NJNEWS14/304270032/6th-bomb-threat-at-Union-County-College-evacuates-Cranford-campus

30. *April 26, WMBF 32 Myrtle Beach* – (South Carolina) **CFHS sees second bomb threat after six arrests and felony charges.** Carolina Forest High School in Myrtle Beach, South Carolina, was evacuated for the second day in a row, April 26, following a bomb threat at the school. Students also evacuated the school the day before because of another threat, and six students were arrested and charged in connection to that threat by the end of the day. According to a Horry County Schools spokesperson, a bomb threat was discovered on a restroom wall April 26. Students were evacuated and allowed back in about 30 minutes later. In addition to being the second bomb threat for Carolina Forest High School in as many days, the April 26 threat was the third consecutive threat in a Horry County school the week of April 23. The other threat was April 24 at Socastee High School. Horry County schools have seen 16 bomb threats in total over the past 5 months. Horry County police arrested six students for the threat April 25. Investigators used surveillance video from the halls to help them figure out who left the threat on a note in the bathroom. Police have not made any arrests for the bomb threats April 24 or April 26.

Source: http://www.wmbfnews.com/story/17792594/cfhs-evacuated-following-second-bomb-threat-is-2-days

31. *April 26, Associated Press* – (Rhode Island) **Father, son indicted in $10M Navy kickbacks case.** A civilian engineer from Virginia who worked for the Naval Sea Systems Command and his father were indicted April 26 in Rhode Island in an alleged bribery and fraud plot that prosecutors said cost the U.S. Navy about $10 million over 15 years. The indictment came after three others accused in the plot pleaded guilty to charges and agreed to cooperate with federal authorities. Prosecutors alleged the son used his authority at the Naval Undersea Warfare Center in Newport, Rhode Island, and his oversight of certain Navy contracts to arrange for naval funds to be funneled back to him directly or through other firms from 1996 until January 2011. Others connected to the son also benefited, prosecutors said. The son faced 33 counts, on charges of conspiracy, bribery, theft of government funds, extortion, wire fraud, and tax evasion. His father faced three counts of tax evasion, prosecutors said. The case prompted an internal Navy investigation that resulted in military officials in Washington D.C. suspending the contracting authority of Newport's Naval Undersea Warfare Center. The Navy said a host of contracting problems at the facility enabled the scheme. The Naval Sea Systems Command announced in October 2011 that it had restored contracting authority to the warfare center, according to a news release.
Source: http://www.google.com/hostednews/ap/article/ALeqM5hL2szaUse6DIR-g4cc1LM0WSxbfQ?docId=1db29d09b3cc41d5872b23726ef020d3

For another story, see item **36**

[Return to top]

Emergency Services Sector

32. *April 26, WWBT 12 Richmond* – (Virginia) **City closes Richmond Juvenile Detention Center.** After a series of mounting concerns related to staff and management shortcomings and allegations of criminal behavior the mayor of Richmond, Virginia, announced April 26 the city of Richmond will close the Richmond Juvenile Detention Center and place most operational staff on administrative leave until further notice. Richmond city youth requiring juvenile detention will be housed at neighboring facilities throughout the surrounding area. The city of Richmond was expected to relinquish its license by close of business April 27. The relocation of residents began April 26. Parents and guardians were notified of the status of the facility and relocation of the juveniles. Employees were given notice and normal human resources procedures were being employed.
Source: http://www.nbc12.com/story/17796157/city-closes-richmond-juvenile-detention-center

For more stories, see items **29** and **40**

[Return to top]

Information Technology Sector

33. *April 27, Softpedia* – (International) **One vulnerable site can serve multiple cybercriminal groups, experts find.** Security researchers found that a single vulnerable Web site may be used by a number of cybercriminal organizations, each one altering the site to serve its own purposes. In many cases, Web sites are compromised and altered to lead visitors to domains that push fake antivirus programs, which lately have become a great way for cyber criminals to earn a profit. A Zscaler expert explained that once the criminals overtake the site, they rely on Blackhat SEO techniques to increase traffic towards their malicious plots. In order to do this, they set up two different pages on the compromised domain. First, they create a spam page that search engines, security scanners, and blacklisting mechanisms see as harmless. This page does not contain obfuscated code and performs the redirect via a PHP or .htaccess file. The second page contains the redirect to a site in charge of performing the attack on users. More recently, researchers identified many overtaken Web sites designed to send users to fake antivirus were also infected with a malicious piece of JavaScript, which held an IFRAME injection that pointed to several different locations.
Source: http://news.softpedia.com/news/One-Vulnerable-Site-Can-Serve-More-Cybercriminal-Groups-Experts-Find-266737.shtml

34. *April 27, H Security* – (International) **PHP 5.4.1 and PHP 5.3.11 released.** The PHP developers released the first update for PHP 5.4, the latest version of their popular scripting language, and an update to PHP 5.3, the older stable branch of the language. The developers said "All users of PHP are strongly encouraged to upgrade" to the new releases. PHP 5.4.1 has more than 20 bug fixes, including some related to security. One security bug concerned insufficient validating of the upload name, which then led to corrupted $_FILES indices. Another notable change was open_basedir checks being added to readline_write_history and readline_read_history. The PHP 5.3.11 upate fixes nearly 60 bugs including correcting a regression in a previously applied security fix for the magic_quotes_gpc directive. A new debug info handler was also added to DOM objects, and the developers added support for version 2.4 of the Apache Web server.
Source: http://www.h-online.com/security/news/item/PHP-5-4-1-and-PHP-5-3-11-released-1561184.html

35. *April 27, The Register* – (International) **Ghost of HTML5 future: Web browser botnets.** During a presentation at the B-Sides Conference in London, England, April 25, a senior threat researcher at Trend Micro outlined how HTML5 could be used to launch browser-based botnets and other attacks. The new features in the revamped markup language — from WebSockets to cross-origin requests — could cause major issues for the information security arena and turn browsers such as Chrome and Firefox into complete cybercrime toolkits. Many attack scenarios involve using JavaScript to create memory-resident "botnets in a browser," the researcher warned, which can send spam, launch denial-of-service attacks, or worse. Because an attack is browser-based, anything from a Mac OS X machine to an Android smartphone can run the platform-neutral code, simplifying the development of malware. Creating botnets by luring users into visiting a malicious Web page, as opposed to having them open a booby-trapped file that exploits a security flaw, offers many advantages to hackers. Malicious Web

documents held in memory are difficult to detect with traditional file-scanning antivirus packages, which seek out bad content stored on disk. JavaScript code is also very easy to obfuscate, so network gateways that look for signatures of malware in packet traffic are easy to bypass — and HTTP-based attacks pass through most firewalls.
Source: http://www.theregister.co.uk/2012/04/27/html5/

36. *April 26, InformationWeek* – (International) **VMware breached, more hypervisor source code to come.** Hypervisors — such as VMware ESXi and Xen — provide the platform on which virtualized guest operating systems run, and are therefore a core component of any business's virtual infrastructure. A 2010 study from IBM found that 35 percent of all vulnerabilities in a virtualized environment could be traced to the hypervisor. Those vulnerabilities are cause for concern in the wake of VMware's April 23 confirmation that source code dating to 2003 and 2004 was publicly released by a hacker billing himself as Hardcore Charlie. Furthermore, he said the release was a "sneak peak" of the 300 MB of VMware source code he said is in his possession, which he said will be publicly released May 5. Charlie said he obtained the VMware kernel source code via March attacks against China Electronics Import & Export Corporation.
Source: http://www.informationweek.com/news/security/attacks/232901025

37. *April 26, Threatpost* – (International) **Critical bug reported in Oracle servers.** There is a critical remotely exploitable vulnerability in all of the current versions of the Oracle database server that can enable an attacker to intercept traffic and execute arbitrary commands on the server. The bug, which Oracle reported as fixed in the most recent Critical Patch Update (CPU), is only fixed in upcoming versions of the database, not in currently shipping releases, and there is publicly available proof-of-concept exploit code circulating. The vulnerability lies in the TNS Listener service, which on Oracle databases functions as the service that routes connection requests from clients to the server itself. A researcher said he discovered the vulnerability several years ago and then sold the details of the bug to a third-party broker, who reported it to Oracle in 2008. Oracle credited the researcher for reporting the bug in its April CPU, but he said in a post on the Full Disclosure mailing list the week of April 23 that the flaw was not actually fixed in the current versions of the Oracle database server.
Source: http://threatpost.com/en_us/blogs/critical-bug-reported-oracle-servers-042612

For more stories, see items **11** and **39**

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

38. *April 27, WLUC 6 Marquette* – (Michigan) **Verizon Wireless service outages.** Verizon Wireless was having outages in parts of the central and western Upper Peninsula of Michigan April 27, according to the Michigan State Police. Service started returning to areas around 10:30 a.m. Call service seemed to be impacted, but data and text was working during the outage.
Source:
http://www.uppermichiganssource.com/news/story.aspx?list=~\home\lists\search&id=747093#.T5rEDNkwJI4

39. *April 26, IDG News Service* – (International) **Engineers look to fix Internet routing weakness.** Information technology engineers are studying what may be an easier way to fix a long-existing weakness in the Internet's routing system that has the potential to cause major service outages and allow hackers to spy on data, IDG News Service reported April 26. The problem involves the routers used by every organization and company that owns a block of Internet Protocol (IP) addresses. Those routers communicate constantly with other routers, updating internal information — often upwards of 400,000 entries — on the best way to reach other networks using a protocol called Border Gateway Protocol (BGP). Changes in that routing information are distributed quickly to routers around the world in as few as 5 minutes. But the routers do not verify the route "announcements," as they are called, are correct. Mistakes in entering the information — or a malicious attack — can cause a network to become unavailable. It can also cause, for example, a firm's Internet traffic to be circuitously routed through another network it does not need to go through, opening the possibility the traffic could be intercepted. The attack is known as "route hijacking," and cannot be stopped by any security product. The solution is to have routers verify the IP address blocks announced by others' routers actually belong to their networks.
Source:
http://www.computerworld.com/s/article/9226657/Engineers_look_to_fix_Internet_routing_weakness?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Read

40. *April 26, San Juan Journal* – (Washington) **Telephone and cellular phone service restored on Orcas.** Telephone systems were back up and running on Orcas Island in Washington State April 26, according to the county Department of Emergency Management (DEM). Telephone connections, as well as cellular phone systems, went down early April 26 on Orcas. Century Link reportedly fixed failures in its systems by early the afternoon of April 26, the DEM said. While phone systems were inoperable, the Orcas Island Fire Department and local team of amateur radio operators handled 9-1-1 calls after the outage interrupted emergency calls on Orcas to the sheriff's department headquarters in Friday Harbor.
Source: http://www.sanjuanjournal.com/news/149146835.html

For another story, see item **35**

[Return to top]

Commercial Facilities Sector

41. *April 26, Austin American-Statesman* – (Texas) **Police say teen sets off 'acid bomb' inside Wienerschnitzel restaurant.** Two teens faced felony charges after police say they set off a homemade "acid bomb" inside a Wienerschnitzel fast food restaurant in Austin, Texas, April 24. Their arrest affidavits said someone at the restaurant called 9-1-1 to say they saw someone "set something off" inside the bathroom. That person then ran away and got into a car and fled. Officers pulled over a car that matched the witnesses' description, the affidavit said. Inside, they found a piece of PVC pipe they believed might have been a pipe bomb. Bomb squad investigators determined the item was not explosive, but found a bag containing six empty plastic bottles with aluminum foil inside and several bottles of bathroom cleaner, the affidavit said.
Source: http://www.statesman.com/blogs/content/shared-gen/blogs/austin/blotter/entries/2012/04/26/police_say_teens_set_off_acid.html

[Return to top]

National Monuments and Icons Sector

42. *April 26, Ionia Sentinel-Standard* – (Michigan) **Wildfire on Huron National Forest 100 percent contained.** The U.S. Department of Agriculture Forest Service determined a 1,400-acre wildfire on the Huron National Forest south of Mio, Michigan, was 100 percent contained as of April 26. The wildfire was first reported April 25 by a passerby and very quickly spread across several hundred acres, forcing the evacuation of many homes near Mack Lake, south of Mio. By the next morning, the fire stretched across 1,436 acres. Firefighting crews from the Forest Service, the Michigan Department of Natural Resources, and the Tri-town Volunteer Fire Department responded. Michigan State Police and the Oscoda County Sheriff's Department closed roads and notified residents of the evacuation. The Red Cross provided assistance to the evacuees in Mio. Although the wildfire was contained, the fire danger remained high because of weather conditions anticipated in the areas. A Type II fire team was mobilized to monitor the burn area for hot spots and potential ignitions due to predicted high winds and warmer weather. The cause of the wildfire remained under investigation by law enforcement officers from the Forest Service and the Michigan Department of Natural Resources.
Source: http://www.sentinel-standard.com/newsnow/x272268267/Wildfire-on-Huron-National-Forest-100-percent-contained

[Return to top]

Dams Sector

43. *April 27, Canberra Times* – (International) **Floods lift dam cost to $405m.** The estimated cost of building the enlarged Cotter Dam in Canberra, Australia, reached $405 million as a result of damage caused by March floods. Actew Corporation revealed record-breaking rains added $17 million to the project, $9 million of which it

will recoup through insurance. However, the government-owned corporation said the impact on consumers will not be known until the independent competition and regulatory commission makes its water price determination in May 2013. Construction will resume at the site May 5. Inspections following the flood found the dam wall held up well, with very little damage to the structure itself. Damage to the tower cranes, plant, and machinery on top of the wall was less than expected.
Source: http://www.canberratimes.com.au/act-news/floods-lift-dam-cost-to-405m-20120426-1xodx.html

44. *April 27, WALB 10 Albany* – (Georgia) **Another bomb found at the dam.** Georgia Bureau of Investigations (GBI) agents were working to figure out who left a bomb at the Georgia Power Dam in Albany, Georgia, April 26. Dougherty County police reported the explosive was found at the bottom of the boat ramp and called the GBI Bomb Squad to diffuse it. This is the second explosive found at the dam in recent weeks. Earlier this month, a man was arrested for having explosives near the dam.
Source: http://www.walb.com/story/17835068/this-is-the-second-time-in-weeks-a-bomb-was-found-at-the-dam

[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