Daily Open Source Infrastructure Report
21 February 2012

Top Stories

- Italian prosecutors said they seized a record $6 trillion of allegedly fake U.S. Treasury bonds and arrested eight people in connection with an organized crime probe. – *Bloomberg* (See item **10**)
- A terrorism suspect was arrested in an FBI sting operation near the U.S. Capitol while planning to detonate what he thought were explosives in Washington D.C. – *Associated Press* (See item **31**)

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. *February 16, Science News* – (Colorado) **Natural gas wells leakier than believed.** Wells that pump natural gas from the ground in Colorado have leaked about twice as much gas into the atmosphere as previously thought, a new study found, Science News reported February 16. A team of atmospheric scientists at the National

Oceanic and Atmospheric Administration and the University of Colorado Boulder monitored air quality southwest of the Denver-Julesburg Basin, an area that feeds more than 20,000 natural gas wells. When winds blew in from the basin, levels of methane detected by sensors on the tower spiked. Landfills, cattle feedlots, and wastewater treatment plants probably belched some of the gas into the sky. However, methane from gas wells was accompanied by other components that allowed it to be fingerprinted and separated out in the analysis. These measurements suggested that about 4 percent of the methane in the gas wells was leaking. Previous studies by the Environmental Protection Agency and by industry groups pegged this loss at between 1 and 2 percent. However, the earlier estimates were done by measuring leakages from individual pieces of equipment. The findings will be reported in the upcoming issue of the Journal of Geophysical Research. The Western Energy Alliance in Denver said gas wells in the area have already made some changes since the data used in the new study were collected that should cut down on leakage.
Source:
http://www.sciencenews.org/view/generic/id/338505/title/Natural_gas_wells_leakier_than_believed

For more stories, see items **27** and **36**

[Return to top]

Chemical Industry Sector

2. *February 16, Minnesota Pollution Control Agency* – (Minnesota) **Northshore Mining to pay $240,175 penalty for air-quality violations.** Northshore Mining Co. agreed to pay a $240,175 penalty to the Minnesota Pollution Control Agency (MPCA) for air-quality violations the MPCA said occurred at the company's taconite-processing plant in Silver Bay, Minnesota, according to a February 16 press release from the MPCA. The violations were for emissions of excessive amounts of very fine dust that is unhealthy to breathe. Northshore is also taking steps to prevent future violations, including emission-control improvements at its large taconite pellet storage yard. Between November 2010 and May 2011, ambient air quality monitors located between the taconite pellet storage yard and the Silver Bay marina measured violations of permit limits for particulate matter, or dust, smaller than 10 microns (PM10) in width. Dust deposits were also documented at the Silver Bay marina. The agency calculated that nearly 30 air-quality violations occurred on monitored days and on days when no monitoring was conducted. Northshore has taken corrective actions to limit and control dust emissions, including increased use of water cannons and other water sprays used for dust control during the transfer and stockpiling of taconite pellets, pellet screening, and in the truck dump area. The company has also increased its use of chemical dust suppressants. Northshore will also mulch exposed areas in the pellet yard, and provide additional dust-control training for its workers.
Source: http://www.pca.state.mn.us/index.php/about-mpca/mpca-news/current-news-releases/northshore-mining-to-pay-$240175-penalty-for-air-quality-violations.html

3. *February 16, Mississippi Press* – (Mississippi) **EPA orders Mississippi Phosphates to correct corrosive water issue at Pascagoula plant.** Mississippi Phosphate Corp. is being ordered by the Environmental Protection Agency (EPA) to take immediate action on a corrosive water issue discovered in 2011 at a Pascagoula, Mississippi facility, the agency announced February 16. Mississippi Phosphates manufactures sulfuric acid and phosphoric acid to produce diammonium phosphate fertilizer. "EPA believes that an imminent and substantial endangerment to human health and the environment exists at the facility due to corrosive water discovered by the facility outside the west stack perimeter dike in January 2011 and September 2011," the EPA said. The order also directs Mississippi Phosphates to continue the corrective actions included in a previous September 2009 order. Under the latest order, Mississippi Phosphates will be required to submit a revised plan to repair and replace degraded containment around sulfuric acid plants; continue to implement the groundwater investigative and remediation work plan for the sulfuric acid plants, DAP plant, and construction area southwest of sulfuric acid plants; complete a daily visual assessment of seepage from west stack perimeter dike; and submit a west gypsum stack system improvement plan.
   Source: http://blog.gulflive.com/mississippi-press-news/2012/02/epa_orders_mississippi_phospha.html

4. *February 15, American Chemical Society* – (National) **Dust from industrial-scale processing of nanomaterials carries high explosion risk.** With expanded industrial-scale production of nanomaterials fast approaching, scientists are reporting indications that dust generated during processing of nanomaterials may explode more easily than dust from wheat flour, cornstarch, and most other common dust explosion hazards, according to a February 15 release from the American Chemical Society (ACS). Their article in ACS' journal Industrial & Engineering Chemistry Research indicates that nanomaterial dust could explode due to a spark with only 1/30th the energy needed to ignite sugar dust — the cause of the 2008 Portwentworth, Georgia, explosion that killed 13 people, injured 42 people, and destroyed a factory. After reviewing results of studies that exist on the topic, the researchers concluded that the energy needed to ignite nanomaterials made of metals, such as aluminum, is less than 1 mJ, which is less than 1/30th the energy required to ignite sugar dust or less than 1/60th the energy required to set wheat dust aflame. Flocking is often made with a process that generates static electricity, which could set off an explosion of flocculent dust, they point out. And the addition of a flammable gas or vapor to a dust as a hybrid mixture increases the chance that the dust will explode. The researchers warn that precautions should be taken to prevent these materials from exposure to sparks, collisions, or friction, which could fuel an explosion.
   Source: http://portal.acs.org/portal/acs/corg/content?_nfpb=true&_pageLabel=PP_ARTICLEMAIN&node_id=223&content_id=CNBP_029293&use_sec=true&sec_url_var=region1&__uuid=912905f8-dcbd-4315-8799-b3fa9e5e6cec

For another story, see item **26**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *February 17, Reuters* – (National) **NRC seeks info about fuel at 11 U.S. nuclear reactors.** The U.S. Nuclear Regulatory Commission (NRC) said February 17 that it was requesting information from 11 nuclear plants regarding fuel performance during accidents. The NRC said this was not something that presents an immediate safety concern so there was no reason to shut any of the plants. The 11 reactors are located at FirstEnergy's Beaver Valley in Pennsylvania, Exelon's Byron in Illinois, Duke Energy's Catawba in South Carolina and McGuire in North Carolina, American Electric Power's Cook, and Dominion's Kewaunee in Wisconsin. A computer program Westinghouse Electric used has a fundamental flaw in determining how the fuel loses the ability to conduct heat. This phenomenon is known as "thermal conductivity degradation." Because of that error there is a possibility that plants could underestimate how hot their fuel could get in an accident.
   Source: http://www.reuters.com/article/2012/02/17/utilities-nrc-fuel-idUSL2E8DH51920120217

6. *February 16, Minneapolis-St. Paul Star Tribune* – (Minnesota) **Prairie Island nuclear plant chided for a security lapse.** Federal regulators February 16 cited Xcel Energy for an unspecified security lapse at the Prairie Island nuclear station near Red Wing, Minnesota. The Nuclear Regulatory Commission (NRC) sent a letter to Xcel about the violation discovered in an October 2011 inspection. Details were redacted from the letter. An NRC spokeswoman said the public's safety was not threatened by the security problem. However, no details, including its level of significance, will be released to avoid publicizing a security vulnerability, she said. An NRC statement would only say publicly that the violation was "greater than green."
   Source: http://www.startribune.com/business/139470418.html

For another story, see item **10**

[Return to top]

Critical Manufacturing Sector

7. *February 16, Yale University* – (National) **Yale paper finds arsenic supply at highest risk.** A paper by Yale University researchers released February 16 studied the dependability of supplies of key metals involved in the manufacturing of electrical and electronic equipment. Modern technology depends on reliable supplies of a wide variety of materials, but there is increasing concern about the dependability of those supplies, the paper said. The Yale team focused on elements of the geological copper family: copper, arsenic, selenium, silver, tellurium, and gold. All six are technologically important. Of the six metals, arsenic was found to be at the highest risk of supply disruption over the long-term because there is scant interest in mining a poisonous material, with selenium and gold almost as high a risk.
   Source: http://www.eurekalert.org/pub_releases/2012-02/yu-ypf021612.php

8. *February 16, U.S. Department of Labor* – (Indiana) **U.S. Department of Labor's OSHA cites Jeffboat for 9 safety violations after worker fatality at Jeffersonville, Ind., barge manufacturing facility.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) February 16 cited Jeffboat LLC for nine safety violations, including one willful violation, at its Jeffersonville, Indiana facility after a worker was fatally crushed August 19, 2011. That fatality was the third at the barge manufacturing facility since May 2010. The OSHA has conducted five inspections since that time, resulting in citations for 46 violations, including the 9 from the most recent investigation. The willful citation is composed of two grouped violations. The first grouped violation is for failing to properly assemble and install pendant controllers used to operate transfer cars in accordance with instructions provided by the manufacturer. The improper installation allegedly allowed water and moisture to enter the pendant controllers, which may have caused the malfunction from the resulting corrosion. The second grouped violation is for continuing usage of equipment for which the electrical parts are corroded. Seven serious violations were also cited.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=21831

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

9. *February 17, Bloomberg* – (Texas; National) **D.R. Horton says loan applicants' personal data was compromised.** D.R. Horton Inc. (DHI), the largest U.S. homebuilder by volume, said it is notifying mortgage applicants that their personal data may have been compromised by a software security infringement, Bloomberg reported February 17. The breach was caused by "unknown external sources," the Fort Worth, Texas-based company said in a statement February 16. It was discovered February 10 at the builder's Internet Loan Prequalification System, according to a message being sent to customers. "DHI Mortgage has already contacted law enforcement and implemented revised online security measures as we continue to investigate the matter," D.R. Horton said in the message. The homebuilder did not say in its statement how many people were affected by the security breach. Information that applicants submitted to D.R. Horton may include birth dates, Social Security numbers, and such financial data as income, assets and liabilities, the company said. D.R. Horton sold 17,176 homes in 25 states in 2011 at prices ranging from $90,000 to more than $600,000. Its in-house mortgage company handled the financing for 60 percent of homebuyers in the quarter that ended December 31, 2011.

Source: http://www.businessweek.com/news/2012-02-17/d-r-horton-says-loan-applicants-personal-data-was-compromised.html

10. *February 17, Bloomberg* – (International) **Record $6 trillion of fake U.S. bonds seized.** Italian anti-mafia prosecutors said they seized a record $6 trillion of allegedly fake U.S. Treasury bonds, an amount that is almost half of the U.S.'s public debt, Bloomberg reported February 17. The bonds were found hidden in makeshift compartments of three safety deposit boxes in Zurich, Switzerland, prosecutors from the southern city of Potenza said in an e-mailed statement. The Italian authorities arrested eight people in connection with the probe. The U.S. embassy in Rome examined the securities dated 1934, which had a nominal value of $1 billion a piece, they said in the statement. The financial fraud uncovered by the Italian prosecutors in Potenza includes two checks issued through HSBC Holdings Plc in London for 205,000 pounds ($325,000), checks that were not backed by available funds, the prosecutors said. As part of the probe, fake bonds for $2 billion were also seized in Rome. The individuals involved were planning to buy plutonium from Nigerian sources, according to phone conversations monitored by the police. The fraud posed "severe threats" to international financial stability, the prosecutors said in the statement. Phony U.S. securities have been seized in Italy before and there were at least three cases in 2009. Italian police seized phony U.S. Treasury bonds with a face value of $116 billion in August of 2009 and $134 billion of similar securities in June of that year.
Source: http://www.bloomberg.com/news/2012-02-17/italy-police-seize-6-trillion-of-fake-u-s-treasury-bonds-in-switzerland.html

11. *February 17, Bloomberg* – (New York; Florida) **Three insurance agents charged in $100 million fraud scheme.** Three insurance agents based in New York and Florida were charged February 16 with using straw buyers to obtain more than $100 million in life insurance policies they resold to third-party investors. The three agents were charged with conspiracy, fraud, and obstruction of justice, the U.S. attorney in Manhattan said in a statement. They each face as long as 80 years in prison if convicted, he said. The three recruited elderly clients of "modest means" to apply for life insurance policies without disclosing to the insurance companies that they intended to sell the policies to investors, according to prosecutors. They earned millions of dollars in commission and purchased some of the policies from the straw buyers for themselves, prosecutors said.
Source: http://www.businessweek.com/news/2012-02-17/three-insurance-agents-charged-in-100-million-fraud-scheme.html

12. *February 17, U.S. Securities and Exchange Commission* – (National) **SEC charges Oregon-based expert consulting firm and owner with insider trading in technology sector.** The Securities and Exchange Commission (SEC) February 17 charged a man and his Portland, Oregon-based expert consulting firm Broadband Research Corporation with insider trading. The charges stem from the SEC's ongoing investigation of insider trading involving expert networks. The SEC alleges that the owner and Broadband claimed to be in the business of providing clients with legitimate research about publicly-traded technology companies but instead typically tipped clients with material nonpublic information that the owner obtained from prohibited

sources inside the companies. Clients then traded on the inside information. Portfolio managers and analysts at prominent hedge funds and investment advisers paid the owner and Broadband significant consulting fees for the information they provided. The owner in turn compensated his sources with cash, meals, ski trips, and other vacations, and even befriended some sources to gain access to confidential information. In a parallel criminal case, the owner has been arrested and charged with one count of securities fraud and one count of wire fraud. The SEC charged 22 defendants in enforcement actions arising out of its expert networks investigation, which uncovered widespread insider trading at several hedge funds and other investment advisory firms. The insider trading occurred in the securities of 12 technology companies — including Apple, Dell, Fairchild Semiconductor, Marvell Technology, and Western Digital — for illicit gains totaling nearly $110 million.
Source: http://www.sec.gov/news/press/2012/2012-30.htm

13. *February 16, U.S. Commodity Futures Trading Commission* – (Texas; International) **Federal court orders Texas resident to pay $31 million for defrauding customers, misappropriating millions of dollars, and providing fictitious records in forex scheme.** The U.S. Commodity Futures Trading Commission (CFTC) February 16 announced that it obtained federal court consent orders resolving its remaining claims against two Houston men, PrivateFX Global One Ltd., SA, and 36 Holdings Ltd. Global One, a corporation formed in Panama, and 36 Holdings are under the control of a court-appointed receiver. The consent orders stem from a CFTC complaint filed in May 2009, charging the defendants with operating a multi-million dollar fraudulent off-exchange foreign currency (forex) scheme. One consent order requires one of the men, Global One, and 36 Holdings jointly and severally to pay $21 million in disgorgement, and orders the man to pay a $10 million civil monetary penalty. The other consent order requires the second man to pay $414,723 in disgorgement and a $140,000 civil monetary penalty. An earlier order found that on or about July 1, 2006, defendants began soliciting investors to purchase shares of Global One, whose purported objective was to speculate in the forex markets. Global One's offering raised approximately $21 million from at least 80 investors by touting Global One's purportedly successful forex trading performance, according to the order. From April 2006 through April 2009, the defendants reported monthly returns, purportedly generated through forex trading, however the defendants' representations to investors regarding Global One's extraordinary forex trading profits and returns were false. The earlier consent order also found that the defendants provided the CFTC with fictitious third-party bank and forex trading records to conceal the fraud. In a related criminal matter, one of the men previously pleaded guilty to one count of securities fraud and was sentenced to 20 years in prison.
Source: http://www.cftc.gov/PressRoom/PressReleases/pr6181-12

14. *February 16, U.S. Department of Treasury* – (International) **Treasury designates Iranian Ministry of Intelligence and Security for human rights abuses and support for terrorism.** The U.S. Department of the Treasury February 16 announced the designation of the Iranian Ministry of Intelligence and Security (MOIS), Iran's primary intelligence organization, for its support to terrorist groups as well as its central role in perpetrating human rights abuses against the citizens of Iran and its role in supporting

the Syrian regime as it continues to commit human rights abuses against the people of Syria. The February 16 actions were taken in consultation with the Department of State and other agencies, as applicable, pursuant to Executive Orders (E.O.) 13224, 13553, and 13572, which target terrorists and their supporters and those responsible for human rights abuses in Iran and Syria, respectively. Any property or property interests in the United States or in the possession or control of U.S. persons in which the MOIS has an interest are blocked, and U.S. persons are prohibited from engaging in transactions with it.
Source: http://www.treasury.gov/press-center/press-releases/Pages/tg1424.aspx

15. *February 16, Associated Press* – (Idaho; Utah) **Former Idaho couple indicted for mortgage fraud.** A federal grand jury in Boise, Idaho, indicted two former Idaho residents on 17-counts of financial fraud and making false statements on mortgage applications, the Associated Press reported February 16. Federal prosecutors also accused the couple of wire fraud and bankruptcy fraud. The charges stem from an investigation into Crestwood Construction and Crestwood Inc., companies engaged in remodeling and reselling homes in Utah and Idaho. The indictment alleges that between February 2005 and March 2007 the couple made false statements on 30 mortgage loans worth $8 million. Prosecutors claim the couple inflated their monthly income, and that those fraudulent documents caused significant losses for banks. Nine people were sentenced in separate cases related to the investigation.
Source: http://www.kivitv.com/news/local/139453608.html

16. *February 16, Dallas Morning News* – (Texas) **Four more convicted in former Dallas Cowboy's massive mortgage fraud scheme.** Four more people have been convicted in a multimillion-dollar mortgage fraud scheme involving a former Dallas Cowboys linebacker. After the former Cowboys player and other defendants pleaded guilty in 2011, the February 16 convictions bring the number of people found guilty of conspiring to trick lenders into issuing risky mortgages to 10. The four face maximum sentences from 20 to 30 years on various counts of wire fraud, bank fraud, or conspiracy. Using business names like Cowboys Mortgage, prosecutors said, the group recruited "straw borrowers," inflated house prices, and falsified information on dozens of north Texas mortgage applications between 2002 and 2005 — netting about $20.5 million in fraudulent loans.
Source: http://crimeblog.dallasnews.com/archives/2012/02/four-more-convicted-in-former.html

[Return to top]

Transportation Sector

17. *February 16, Associated Press* – (New Jersey) **NJ trooper's triplets in bus crash; 1 dead, 2 hurt.** A dump truck collided with a bus carrying elementary schoolchildren February 16, killing a daughter of a state trooper and critically injuring three other students — two of them the triplet sisters of the dead girl, authorities said. The accident occurred at a four-way intersection in Chesterfield, New Jersey, a town south of Trenton. It sent the bus, which was carrying 25 students, crashing sideways into a

traffic signal pole, crumpling the side. Police said 17 students received injuries, most of them minor. A Chesterfield police chief said the bus had a stop sign while the dump truck had a flashing yellow light. He said it was unclear whether the bus was attempting to cross the intersection or turn when the collision happened. The dump truck ran off the road into a grassy area. Police said the investigation was incomplete.
Source: http://www.times-standard.com/ci_19978803

18. *February 16, Baltimore Sun* – (Maryland) **Driver of truck that crashed, leaked additive charged with DWI.** The driver of a tractor-trailer that crashed on southbound Interstate 95 (I-95) outside of Baltimore February 15 has been charged with driving while impaired by alcohol, police said. The driver crashed a semitrailer on an overpass above Interstate 895 (I-895), turning the truck over in the left lane of I-95, just north of the Harbor Tunnel, according to a spokesman for the Maryland Transportation Authority Police. The truck was carrying 13 containers that each held 275 gallons of a water-based additive for concrete. Two containers fell off the overpass, landing on I-895, which was temporarily closed while tunnel lanes changed direction, the police spokesman said. The concrete additive, which was not hazardous, and diesel fuel spilled from the truck and dripped onto cars as they passed under I-95. Southbound I-95 was closed for more than 7 hours while the spill was removed. Both directions of I-895 were closed for over 4 hours.
Source: http://articles.baltimoresun.com/2012-02-16/news/bs-md-ci-dwi-charge-20120216_1_additive-tunnel-lanes-truck

19. *February 15, Knoxville News Sentinel* – (Tennessee) **Overloaded trailer splits in two on Strawberry Plains Pike.** A big-rig's overloaded trailer snapped in two while being hauled along Strawberry Plains Pike in Knoxville, Tennessee, February 15. The 1996 International tractor-trailer, operated by Rock Island Express, was hauling approximately 45,000 pounds of coiled steel when the accident occurred near the Interstate 40 interchange, according to the Knoxville Police Department. The trailer split in two under the weight of the steel, leaving the back half — wheels and all — pointed near-vertical off the ground. One southbound lane of Strawberry Plains Pike was blocked while a local towing company attempts to unload the trailer. The pike's northbound turn lane to I-40 westbound also was blocked.
Source: http://www.knoxnews.com/news/2012/feb/15/overloaded-trailer-splits-in-two-on-strawberry/?partner=RSS

For another story, see item **27**

[Return to top]

Postal and Shipping Sector

20. *February 17, Associated Press* – (Delaware) **Del. post office evacuated because of suspicious package; 1 taken to hospital.** A suspicious package in Wilmington, Delaware, led to the evacuation of a post office and another building, and some roads were closed February 17. New Castle County paramedics told the News Journal of Wilmington that one person was taken to a hospital and several others were treated at

the scene.
Source: http://www.therepublic.com/view/story/266a12bd88a2416cad9b862d7603e361/DE--Suspicious-Package/

21. *February 16, Ridgewood-Glen Rock Patch* – (New Jersey) **Mail carrier charged with DWI in postal truck.** A post office employee delivering mail was arrested on charges of drinking and driving February 16 in Ridgewood, New Jersey, police said. Police allege the employee was drunk and had an open container of alcohol in the postal vehicle while on her delivery route February 16. She was pulled over and subsequently arrested and charged with DWI, being under the influence of a controlled dangerous substance, and possessing an open container, the Ridgewood Police captain said. The employee has been placed on non-paid "emergency suspension status" pending the outcome of investigation.
Source: http://ridgewood.patch.com/articles/mail-carrier-charged-with-dwi-in-postal-truck

[Return to top]

Agriculture and Food Sector

22. *February 17, Food Safety News* – (Massachusetts) **MA firm recalls chili for lack of inspection.** A Massachusetts-based company is recalling approximately 3,800 pounds of chili products because they may not have undergone federal inspection. The Chili Station, located in Ludlow, Massachusetts, voluntarily recalled containers of its beef and turkey chili February 16. The chili products were distributed and sold in Massachusetts. The problem was discovered during a routine Food Safety Assessment conducted by FSIS.
Source: http://www.foodsafetynews.com/2012/02/ma-company-recalls-chili-for-lack-of-inspection/

23. *February 17, Food Safety News* – (National) **Raw milk Campylobacter outbreak expands.** An additional Campylobacter infection brought the total number of illnesses to 77 in an outbreak linked to raw milk from Your Family Cow dairy in Chambersburg, Pennsylvania. The Pennsylvania Department of Health reported the additional illness February 16, according to CIDRAP. The outbreak began at the end of January. Since that time, at least 9 people have been hospitalized. The new breakdown of illnesses by state is as follows: Pennsylvania (67 illnesses), Maryland (5), West Virginia (3), and New Jersey (2).
Source: http://www.foodsafetynews.com/2012/02/raw-milk-campylobacter-outbreak-expands/

24. *February 17, Food Safety News* – (International) **FDA updates information on fungicides in OJ.** The Food and Drug Administration (FDA) published a new update February 16 to its ongoing testing of imported orange juice for the fungicide carbendazim, a compound restricted from agriculture in the United States. Since January 9, the FDA has tested samples from 104 shipments of orange juice and orange

juice concentrate. Out of those, the agency found 24 shipments that contained at least 10 parts per billion (ppb) of carbendazim. Half of those 24 shipments came from Canada, while the other half came from Brazil. Of the shipments testing negative for carbendazim, 57 have been released for sale. The FDA began testing all orange juice imports for carbendazim in January after being alerted by Coca Cola — owner of Minute Maid and Simply Orange — that some juice from Brazil had tested positive for the fungicide. The Environmental Protection Agency considers carbendazim levels below 80 ppb safe for human consumption. In earlier tests of shipments, those containing the fungicide ranged in concentration from 13 to 36 ppb. The FDA will not allow sale of any shipments containing more than 10 ppb.
Source: http://www.foodsafetynews.com/2012/02/fda-updates-information-on-fungicides-in-oj/

25. *February 17, Ocean City Today* – (Maryland) **Millsboro man charged with metal theft from Perdue Farms.** A man was charged February 12 in connection with the theft of metal from the former Showell, Maryland facility of Perdue Farms. Maintenance personnel documented the thefts, which took place during the period of a few weeks. The HVAC units on the building's roof were stripped of copper and aluminum and several cooling fans and duct work for chillers were taken, as well as a ground-based York air conditioning unit, the Worcester County Bureau of Investigation stated in a press release. Detectives estimated it would cost more than $500,000 to repair the HVAC systems to current standards set by the Environmental Protection Agency. The suspect was charged with malicious destruction of property, theft scheme from $1,000 to $10,000, and two counts of theft from $1,000 to less than $10,000.
Source: http://www.oceancitytoday.net/news/2012-02-17/Police/Millsboro_man_charged_with_metal_theft_from_Perdue.html

26. *February 17, Charleston Gazette* – (West Virginia) **Nine sent to hospital after chemical exposure at IHOP.** Nine workers at the IHOP restaurant in the Shops at Trace Fork in South Charleston, West Virginia, were taken to the hospital February 17 after workers mixed chemicals and released a cloud of hazardous material into the air. About 50 people were inside the restaurant when an employee added the wrong chemical to a dishwasher that is used to clean restaurant hardware. A South Charleston Fire Department captain said the two chemicals — a degreaser and a chlorine-based cleaner — are used in routine cleaning at the restaurant and were mixed together in a way that created a "hazardous air quality." After calling 9-1-1, restaurant workers evacuated diners and moved everyone outside the building.
Source: http://wvgazette.com/News/201202170049

[Return to top]

Water Sector

27. *February 17, CNN* – (Louisiana; Mississippi) **Barge collision spills oil into the Mississippi.** A barge collision near New Orleans spilled oil into the Mississippi River February 17, and prompted authorities to close a five-mile stretch of the waterway. The St. Charles Parish Department of Waterworks shut down both of its water intakes

located in New Sarpy and Luling due to the spill but said the incident did not pose a public threat. Response agencies were on the scene. Two barges ran into each other near Reserve in St. John Parish, west of New Orleans. A U.S. Coast Guard official said an investigation team has been dispatched and is taking images from the air to further assess the gravity of the situation.
Source: http://www.cnn.com/2012/02/17/us/louisiana-oil-spill/index.html

28. *February 17, KXLY 4 Spokane* – (Washington) **Water main break closes road, damages homes.** A massive water main break in North Spokane, Washington flooded a neighborhood and caused water damage to several homes. The water main broke on the corner of Wellesley and Perry February 16. A spokesman for the City of Spokane Water Department estimated the water main break spilled between 100,000 and 500,000 gallons of water into the streets. Almost an hour after the break, city water crews stopped the water and started working to repair the line. Firefighters waded through the knee deep water as well to clear drains. Wellesley from Crestline to Nevada was closed overnight to repair the line and fix the road. At least two homes received water damage. The water department spokesman said there was a report of a water main leak in the area February 15, but could not say if it was the same line that burst February 16.
Source: http://www.kxly.com/sports/30480059/detail.html

29. *February 16, Associated Press* – (Colorado) **Red Cliff seeking federal aid for water emergency.** The mayor of Red Cliff, Colorado, is hoping the federal government will help with some of the costs of coping with a water emergency that shut off water to the town. The mayor said the town does not have the estimated $60,000 to pay for repairs and hopes the federal government will help out. So far, the city has not filed an official request for financial aid for the four-day shutdown. According to the Vail Daily, some customers had to hire welders to thaw out their pipes. The water district for the community of more than 300 people about 100 miles west of Denver traced the problem to a frozen water main that connects the water plant to the town.
Source: http://www.denverpost.com/breakingnews/ci_19978105

For another story, see item **3**

[Return to top]

Public Health and Healthcare Sector

30. *February 16, WBUR 90.9 FM Boston* – (National) **FDA steps in to avert children's cancer drug shortage.** The U.S. Food and Drug Administration (FDA) has stepped in to help avert an imminent shortage of methotrexate, a drug used to treat childhood blood cancer, after the main supplier of the drug, Bedford Laboratories' Ben Venue factory in Ohio, shut down the fall of 2011 because of production problems. In a statement an FDA spokeswoman sent via e-mail February 16: Bedford advised the FDA that it will release emergency supplies of preservative-free methotrexate to meet patient needs. This additional quantity of medicine was produced before the company voluntarily shut down and the company has worked to ensure that the drug was not

impacted by the issues that led to the plant shutdown. Based on the information provided by the firms, the new supplies are anticipated to be available by the end of this month with ongoing releases in March. USA Today reported that the FDA is also working to secure foreign supplies.
Source: http://commonhealth.wbur.org/2012/02/breaking-fda-steps-in-to-fix-childrens-cancer-drug-shortage/

[Return to top]

Government Facilities Sector

31. *February 17, Associated Press* – (Washington D.C.) **Terror suspect arrested near Capitol in FBI sting.** Police said a terrorism suspect has been arrested in an FBI sting operation near the U.S. Capitol while planning to detonate what he thought were explosives in Washington, D.C. U.S. Capitol Police said their officers and FBI officials arrested the man February 17 in a sting operation. A Justice Department spokesman said the suspect was closely monitored by law enforcement, and the purported explosives were deactivated, so the public was not in danger. Two people briefed on the matter told the Associated Press he was not arrested on the Capitol grounds, and the FBI has had him under surveillance around the clock for several weeks. A U.S. law enforcement official said the person arrested was canvassing the U.S. Capitol with violent intentions. He was not believed to have any known connections to al Qai'da. It was not immediately clear whether he was a U.S. citizen.
Source: http://www.ajc.com/news/nation-world/terror-suspect-arrested-near-1353002.html

32. *February 17, Washington, D.C. Hill* – (National; International) **Anonymous hacks Federal Trade Commission Web sites.** Internet activist group Anonymous hacked two Web sites of the Federal Trade Commission (FTC) February 14 and posted a violent video satirizing the Anti-Counterfeiting Trade Agreement (ACTA). The hackers attacked the FTC's Bureau of Consumer Protection's Business Center and a site promoting the National Consumer Protection Week. The main FTC Web page was unaffected. "The FTC takes these malicious acts seriously," the FTC spokeswoman said in a statement. "The sites have been taken down and will be brought back up when we're satisfied that any vulnerability has been addressed." Both sites were inaccessible February 17. The hackers replaced the government Web sites with a German-language video depicting a man in a ski mask gunning down people for downloading copyrighted music. In a profanity-laced statement, Anonymous promised to "rain torrential hellfire down on all enemies of free speech, privacy and internet freedom" if ACTA is approved.
Source: http://thehill.com/blogs/hillicon-valley/technology/211395-anonymous-hacks-federal-trade-commission-websites

33. *February 17, ARL Now* – (Virginia) **Phone, Internet problems at schools, Central Library.** Phone and Internet service was out at a number of schools and at Arlington Central Library in Arlington, Virginia, February 16. All Internet at the library, including access to the library catalog system, was down. Most Arlington Public

Schools south of Route 50 also experienced the same problems, according to a school employee. Phone and Internet service was down at the schools in the afternoon February 16, around the same time the Central Library lost its phone and data service. In both cases, ARL Now was told a problem with a Comcast fiber optic line was to blame. All services were restored to the Central Library early February 17, a library spokesman said.
Source: http://www.arlnow.com/2012/02/16/phone-internet-problems-at-schools-central-library/

34. *February 16, Hagerstown Herald-Mail* – (Pennsylvania) **Pa. school district to purchase emergency notification system.** The Greencastle-Antrim School District in Pennsylvania needed a district wide emergency notification system for several years, but that need moved to the top of the list following a December 2011 accident involving one of the district's school buses, school officials said February 16. After investigating a number of systems, the district's director of educational operations, recommended that the district purchase the School Messenger emergency notification system. The system would provide phone and e-mail notification to parents and guardians of students in the district regarding any type of district wide emergency, he said.
Source: http://www.herald-mail.com/news/tristate/hm-pa-school-district-to-purchase-emergency-notification-system-20120216,0,6040740.story

35. *February 16, Hartford Courant* – (Connecticut) **CCSU: 18,275 social security numbers exposed.** A security breach in a computer at Central Connecticut State University exposed Social Security numbers of students and of current and former employees to potential risk and misuse, the Hartford Courant reported February 16. A computer in the business office became infected by a "Z-Bot" virus, which exposed 18,275 Social Security numbers, said the university's chief information officer. The university said it was matching numbers with names and addresses and will contact each person who was exposed. The university sent out notifications to the campus community February 16. It is offering free identity protection services for up to 2 years for those whose Social Security numbers were exposed.
Source: http://www.courant.com/community/new-britain/hc-ccsu-breach-0217-20120216,0,6145342.story

36. *February 16, San Jose Mercury News* – (California) **Copper wire thieves leave Fremont with $460,000 in repairs.** The city of Fremont, California, could pay nearly $1.3 million in street light repairs in 2012 following a string of copper wire thefts in recent months, the San Jose Mercury News reported February 16. The Fremont City Council unanimously approved an amendment to its streetlight and public facilities maintenance contract with Republic ITS. The contract, which began in 2008, had an initial 1 year term with a not-to-exceed amount of $576,495 and four 1 year options to renew. The city amended the contract 2 years ago by $60,000 due to additional required work. The contract was amended in 2011 to increase by $200,000. Now in its third option year, the council's approval jumps the not-to-exceed amount to $936,495, an increase of $300,000. However, if additional work is required on the streetlights, the council's approval also authorizes the city manager to further increase the not-to-

exceed amount by another $350,000, for a total of more than $1.28 million. The city's public works director said the increases are due to a rash of copper wire thefts from streetlights that have occurred over the last 2 years. Copper thieves have been breaking into the pull boxes near the light poles, tying the wire to their vehicles and then driving away to see how much wire they can pull. Streetlight copper thefts have increased dramatically since 2010, as the value of copper has increased and vandals try to sell it as scrap metal. In January, the city of San Jose reported 169 incidents of streetlight wire theft since 2010. Likewise, Bay Area Rapid Transit reported wire and cable thefts in the past year resulted in more than $500,000 in equipment and labor costs, and has delayed projects for months, according to staff.
Source: http://www.mercurynews.com/fremont/ci_19981669

For another story, see item **39**

[Return to top]

Emergency Services Sector

37. *February 17, Framingham MetroWest Daily News* – (Massachusetts) **Man indicted for threatening to bomb state police HQ in Framingham.** An Oxford, Massachusetts man accused of threatening to bomb the head of the state police in August 2011 was indicted by a Middlesex County grand jury. He was charged by the grand jury with three counts of making a bomb threat and one count of threatening to commit a crime, the Middlesex district attorney's office said. He is scheduled to be arraigned in Middlesex Superior Court February 21. He repeatedly called the Massachusetts State Police headquarters in Framingham August 22, 2011. During one of the calls, he threatened to throw a bomb at the receptionist who was answering the phone and a lieutenant colonel, police said. Authorities also said that he had previously made several harassing calls to the state police. At his Framingham District Court arraignment, he was released without bail after pleading not guilty. The judge ordered him to stay 50 yards from the state police barracks and told him to not contact the state police, except through his lawyer.
Source: http://www.metrowestdailynews.com/news/x306962761/Man-indicted-for-threatening-to-bomb-state-police-HQ-in-Framingham

38. *February 17, WJXT 4 Jacksonville* – (Florida) **2 Clay County deputies shot, 1 dies.** Two deputies were shot during a raid of a suspected meth lab in Middleburg, Florida, February 16. One of those deputies and a suspect shot as he ran from the scene both died, according to the Clay County sheriff. The second deputy was also hit by gunfire in the incident. The second detective was struck in the arm and was taken to a nearby medical center where he was listed in serious but stable condition. Five people were arrested at the scene, and authorities said at least some of them may have been staying at the house without the knowledge or permission of the owners. The Florida Department of Law Enforcement will be the lead agency in the investigation of the police-involved shooting and will also assist in the clean up of the drug lab.
Source: http://www.news4jax.com/news/2-Clay-County-deputies-shot-1-dies/-/475880/8796158/-/jntoxo/-/index.html?hpt=ju_bn4

39. *February 16, Los Angeles Times* – (California) **FBI probes deadly shooting involving ICE agents in Long Beach.** About 100 FBI agents February 16 were combing a shooting scene in Long Beach, California, where a federal agent had wounded his supervisor before being fatally shot by another agent. The FBI agents were interviewing witnesses and processing the crime scene after the dispute between the agents with the federal Immigrations and Customs Enforcement agency, known as ICE, at the Glenn M. Anderson Federal Building. Multiple law enforcement authorities told the Los Angeles Times the shooting involved a dispute between an agent and his supervisor. The agent opened fire repeatedly on the male supervisor in the building, according to the sources. With the supervisor wounded, a third agent intervened and opened fire on the gunman, who was pronounced dead at the scene, according to law enforcement authorities. The supervisor was taken to a nearby hospital. The Long Beach Police Department, which initially responded to the call, was investigating the shooting with FBI. They were being aided by the ICE office of Professional Responsibility.
    Source: http://latimesblogs.latimes.com/lanow/2012/02/fbi-probes-ice-agent-shooting.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+lanowblog+(L.A.+Now)

40. *February 16, Missoula Missoulian* – (Montana) **Missoula County emergency services 1st in state to get Smart 9-1-1.** Missoula County, Montana, will be the first in the state to go online with a new national database called Smart 9-1-1. People can use the service, which launches February 21, to create personal and household profiles with information such as medical conditions, photos, and their pets - information that would be available to dispatchers when someone calls 9-1-1. Smart 9-1-1, the emergency services director said, could help dispatchers better distinguish accidents from true emergencies. County employees will not be able to see anyone's profile unless that person calls 9-1-1.
    Source: http://missoulian.com/news/state-and-regional/missoula-county-emergency-services-st-in-state-to-get-smart/article_d0b35ef2-5916-11e1-881c-0019bb2963f4.html

For another story, see item **50**

[Return to top]

Information Technology Sector

41. *February 17, Help Net Security* – (International) **Fake Facebook notification delivers keylogger.** Fake Facebook notifications about changes in users' account information have been hitting inboxes and delivering malware to unwary users, warn Barracuda Labs researchers. The e-mail address of the sender is spoofed to make it look like it has been sent by the social network, and the message contains only an image implying that the recipient needs to install Silverlight in order to view the content. Hovering with mouse over the image shows that the offered file is a Windows PIF file, and that is hosted on an IP address in Malaysia. The file is actually a keylogger, the Jorik Trojan. Once the keylogger is installed, it starts recording every keystroke and Web page title

into a disk file, which is ultimately sent to a C&C server operated by cyber criminals.
Source: http://www.net-security.org/malware_news.php?id=2002

42. *February 17, Help Net Security* – (International) **New powerful bot spreads by e-mail.** PandaLabs reported the presence of a powerful new bot called Ainslot.L. This malware is designed to log user activities, download additional malware, and take control of users' systems. Additionally, it acts as a banker Trojan, stealing log-in information related to online banking and financial transactions. Ainslot.L also performs scans on the computer to seek and remove other bots, becoming the only bot on one's system. "What makes this bot different is that it eliminates all competition, leaving the computer at its mercy," explained the technical director of PandaLabs. Ainslot.L spreads via a fake e-mail purporting to come from a UK clothing company called CULT. The message informs users that they have placed an order in the amount of 200 pounds on CULT's online store and the invoice amount will be charged to their credit card. The text includes a link to view the order which actually downloads the bot onto the computer.
Source: http://www.net-security.org/malware_news.php?id=2001

43. *February 16, Government Computer News* – (International) **Android suddenly the top target as mobile malware rises sharply, study finds.** The amount of malicious code written for mobile devices, such as smart phones and tablets, jumped by 155 percent in 2011 and has grown more sophisticated, according to a new report from Juniper Networks' Mobile Threat Center. The magnitude of the growth is surprising, said Juniper's vice president of government affairs and critical infrastructure protection. "It's a direct result of consumer demand." Spyware makes up the bulk of identified mobile malware, accounting for 63 percent. The SMS trojan accounts for 36 percent of mobile malware. The amount of malware written for Android increased exponentially in 2011, going from 400 identified samples in June to more than 13,000 in December. In 2010, more than 70 percent of identified malware was written for Java ME, with another 27 percent for Symbian. BlackBerry, Android, and Windows Mobile accounted for no more than"other." In 2011, Android was the top target, with nearly 47 percent of identified malware, and Java ME had dropped to a still respectable 41 percent. Symbian accounted for 11.5 percent.
Source: http://gcn.com/Articles/2012/02/16/Mobile-malware-Android-top-target.aspx?Page=1

44. *February 16, The Register* – (International) **DNS flaw reanimates revoked sites as ghost domains.** Cyber crooks may be able to keep malicious domains operating for longer — even after they are revoked — by manipulating the Web's Domain Name System (DNS). A weakness in the cache update logic of many widely used DNS servers creates the potential to establish so-called ghost domains, according to a recent joint study by a team of researchers from universities in China and the United States. In their paper Ghost Domain Names: Revoked Yet Still Resolvable, the researchers explain that deleting the malicious domain from the upper level DNS servers is insufficient. Their experiments with 19,045 open DNS servers show that even one week after a domain name has been revoked and its TTL expired, more than 70 percent of the servers will still resolve it. The researchers found that DNS server

implementations by BIND, Microsoft, Google, and OpenDNS are all potentially vulnerable.
Source: http://www.theregister.co.uk/2012/02/16/ghost_domains_dns_vuln/

45. *February 15, Network Computing* – (International) **Cybercriminals building intricate, multiuse malnets.** Cybercriminals have gotten so sophisticated that they can build an intricate network infrastructure and use it repeatedly for the distribution of malware, according to a new study from Blue Coat Systems. These malware networks, or malnets, lure targets through trusted Web sites, then route them to malware through relay, exploit, and payload servers to deliver the malware payload. While malnets are becoming increasingly sophisticated, Blue Coat said these assets can be identified and the malware attacks blocked. However, the Blue Coat Systems 2012 Security Report notes that these malnets are constantly on the move, making them hard to pin down. In one case, in early February, a malware payload changed locations more than 1,500 times in a single day.
Source: http://www.networkcomputing.com/security/232600910

For another story, see item **9**

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

46. *February 16, University of Minnesota* – (International) **University of Minnesota researchers discover that cell phone hackers can track your physical location without your knowledge.** Cellular networks leak the locations of cell phone users, allowing a third party to easily track the location of the cell phone user without the user's knowledge, according a February 16 press release announcing the findings of new research by computer scientists in the University of Minnesota's College of Science and Engineering. Using an inexpensive phone and open source software, the researchers were able to track the location of cell phone users without their knowledge on the Global System for Mobile Communications (GSM) network, the predominant worldwide network. In a field test, the research group was able to track the location of a test subject within a 10-block area as the subject traveled across an area of Minneapolis at a walking pace. The researchers used readily available equipment and no direct help from the service provider. The researchers have contacted AT&T and Nokia with low-cost techniques that could be implemented without changing the hardware, and are in the process of drafting responsible disclosure statements for cellular service providers.
Source: http://www1.umn.edu/news/news-releases/2012/UR_CONTENT_374462.html

47. *February 16, Columbia Missourian* – (Missouri) **KMIZ signal goes down Thursday afternoon.** KMIZ 17 in Columbia, Missouri, went down February 16 after experiencing problems with the station's transmitters. The station cut its signal to all providers in the televising area, except to Mediacom and CenturyLink. The engineers working identified the issue as a malfunction with the "exciter" in the transmitter, which is not a piece of equipment the station keeps readily on hand, KMIZ's general manager said. The part was being shipped overnight, and they hoped to fix the problem first thing the morning of February 17.
Source: http://www.columbiamissourian.com/stories/2012/02/16/kmiz-goes-down-thursday-afternoon/

48. *February 16, SecurityNewsDaily* – (International) **Anonymous vows to shut down the Internet.** Anonymous has threatened to launch Operation Global Blackout (OpGlobalBlackout), which calls for supporters to download a denial-of-service launching tool, called "Ramp," which will flood the 13 root Domain Name Servers (DNS) of the Internet with more requests than they can process, SecurityNewsDaily reported February 16. February 12, an announcement appeared on the file-hosting site Pastebin declaring March 31 as the day "anonymous will shut the Internet down." The manager for Root Zone Services at the Internet Corporation for Assigned Names and Numbers said, "There are not 13 root servers. There are many hundreds of root servers at over 130 physical locations in many different countries." This discrepancy is critical, said a consultant from Errata Security. "The Anonymous hackers can certain(ly) cause local pockets of disruption, but these disruptions are going to be localized to networks where their attack machines are located," he wrote. "They might affect a few of the root DNS servers, but it's unlikely they could take all of them down, at least for any period of time. On the day of their planned Global Blackout, it's doubtful many people would notice."
Source: http://www.msnbc.msn.com/id/46420147/ns/technology_and_science-security/#.Tz57CYGLcdU

For more stories, see items **33** and **44**

[Return to top]

Commercial Facilities Sector

49. *February 17, Salt Lake Tribune* – (Utah) **Salt Lake City firefighters put out Avenues fire.** Firefighters extinguished a large fire February 16 at the Fountain View Apartments in Salt Lake City. A spokesman for the Salt Lake City Fire Department said the fire started in the boiler/maintenance room on top of the four-story building, but was contained to that room and did not spread to any of the apartment units, according to a fire department spokesman. All 24 apartments were evacuated as firefighters fought the fire. The apartment below the boiler room received some water damage, but no apartment suffered any smoke or fire damage. The 35 residents of the apartments were allowed to go back for their belongings, but nobody was permitted to stay overnight in the building.

Source: http://www.sltrib.com/sltrib/news/53534371-78/fire-firefighters-apartment-apartments.html.csp

50. *February 16, New Hampshire Union Leader* – (New Hampshire) **4-alarm blaze likely caused by cigarette; 40 people displaced.** Two firefighters were burned and seven people rescued in a four-alarm fire February 16 at a Manchester, New Hampshire condominium complex. The cause of the fire was likely the improper disposal of a cigarette, according to the fire chief. He said someone tossed the cigarette onto the first-floor balcony of unit 103. The unit is on the front of the attached three-story apartment building. Forty people were displaced from the building.
Source: http://www.newhampshire.com/article/20120216/NEWS07/702169949

[Return to top]

National Monuments and Icons Sector

51. *February 17, Austin American Statesman* – (Texas) **Five-year Lost Pines fire recovery plan expected to cost more than $17 million.** Bastrop County officials estimated that it will cost $17.2 million over the next 5 years to restore the native vegetation on private land that was burned in the wildfires that began the weekend of September 3, 2011 in Texas. "It's an ambitious plan, and I'm optimistic that through the efforts of the recovery team and Bastrop Commissioners Court, we will be successful," said a coordinator of the Lost Pines Recovery Team. The 5 year environmental recovery plan includes erosion control, reseeding native grasses and wildflowers, and planting drought-hardy loblolly pines and native hardwoods on 11,360 acres of private land, and thinning the underbrush that becomes fuel for fire on an additional 5,000 acres. The September 2011 wildfires, which burned 34,000 acres across the county, damaged the ecosystem of the Lost Pines area, deflated private property values, caused the loss of topsoil and forced sediment into the Colorado River. The county requested support of federal agencies.
Source: http://www.statesman.com/news/local/five-year-lost-pines-fire-recovery-plan-expected-2181148.html

52. *February 14, KVOA 4 Tucson* – (Arizona) **Hilton Fire now 100 percent contained.** The Hilton Fire burning in the Empire Mountains in Arizona east of Highway 83 was 100 percent contained as of February 14, officials confirmed. The fire, which started on February 11, grew to about 460 acres, burning in the vicinity of Hilton Ranch Road, south of Vail, Arizona. The fire spread to public land administered by the Bureau of Land Management and private land. Officials said the fire was human-caused and is still under investigation.
Source: http://www.kvoa.com/news/hilton-fire-now-100-percent-contained/

[Return to top]

Dams Sector

53. *February 17, KJRH 2 Tulsa* – (Oklahoma) **$22 million needed to repair aging levee system.** Tulsa County, Oklahoma, needs about $20 million to fix the aging Tulsa/West Tulsa levee system, KJRH 2 Tulsa reported February 17. The levee system was deemed "unacceptable" by FEMA in 2008. An "unacceptable" rating does not mean the thousands of residents who live along the Arkansas River are in any immediate danger. It means the levee system has a couple of deficiencies within it that could prevent it from working the way it was designed to in the event of a major flood. The federal government ordered local officials to make significant progress in repairing the levee system within a few years. However, the federal government did not provide any funding for those repairs. "We need about $22 million dollars and the Corp. has come up with about $100,000 to do a study to see exactly what we need to do to make the levee viable," an official said.
Source: http://www.kjrh.com/dpp/news/local_news/20-million-needed-to-repair-agin-levee-system

54. *February 16, San Diego Union-Tribune* – (California) **Lake Wohlford to get a new dam.** A new dam to replace one that at risk for collapse, is being planned for Lake Wohlford in Escondido, California, the San Diego Union-Tribune reported February 16. The lake sits about 900 feet above and a couple miles east of Escondido. If filled, it could hold more than 2 billion gallons of water held back by a dam that was built 112 years ago. If the dam somehow burst, a good part of the city would find itself under water rather quickly. For decades the dam passed state testing requirements, but about 5 years ago tests determined that in a major earthquake the part of the dam added in 1924, might fail. Authorities almost immediately lowered the water level so that the lake came up only to the stable part of the dam. Now the city plans on replacing the old dam with a new one to be built a bit downstream. Or, depending on what studies find is most feasible and cost effective, perhaps the old dam will simply be rebuilt replacing the top part with more sturdy material.
Source: http://www.utsandiego.com/news/2012/feb/16/lake-wohlford-get-new-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/iaipdailyreport

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