Daily Open Source Infrastructure Report
5 March 2012

Top Stories

- The entire town of Medford, Oklahoma, was urged to evacuate March 1 as propane from a storage plant leaked for a third straight day, leading to a major fire hazard. – *Associated Press* (See item 2)
- The growing popularity of tax preparation software led to a marked increase in e-mail scams targeted at do-it-yourself taxpayers during the 2012 tax season. – *USA Today* (See item 18)
- SWAT officers in Buena Park, California, rescued a bank manager held at gunpoint by an accused robber March 1. The accused robber was arrested after being wounded in a shootout that also injured some officers. – *Associated Press* (See item 21)
- A researcher presented evidence at a technology conference showing thousands of embedded Web servers on printers, fax machines, and video conferencing systems could be accessed via the Internet. – *H Security* (See item 48)
- Powerful storms that produced tornadoes stretching from the Gulf Coast to the Great Lakes flattened scores of buildings in several states and wiped out a small Indiana town. – *Associated Press* (See item 57)

Fast Jump Menu

Energy Sector

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

1. *March 2, Associated Press* – (National) **Gulf oil spill response consortium better equipped.** A consortium set up by major oil companies to clean up offshore oil spills by quickly marshaling boom and skimmers said it has expanded its resources, the Associated Press reported March 2. The New Orleans Times-Picayune reported the Marine Spill Response Corp. (MSRC) now has 7 response vessels and that it has bought more than 21,000 feet of boom. The MSRC also said it is better prepared to deploy chemical dispersants to break up spilled oil and that is has developed better oil-burning operations. The MSRC, founded in 1990, is funded by oil companies such as BP, Chevron, ExxonMobil, ConocoPhillips, and Shell.
Source: http://www.wlbt.com/story/17064306/gulf-oil-spill-response-consortium-better-equipped

2. *March 1, Associated Press* – (Oklahoma) **Officials urge evacuation of Okla. town as propane leak at fuel storage plant enters 3rd day.** Residents of Medford, Oklahoma, were urged to evacuate March 1 as propane leaked for a third straight day out of a well at a fuel storage plant, and officials feared there could be a fire hazard if strong winds carry the vapor into town. “The issue is propane will settle in low-lying areas,” the Medford city manager said. “If there is any kind of spark or ignition then it would be flammable and could start a fire.” The leak began February 28 when a saltwater brine mixture used to move the propane out of a well at the plant spilled, causing propane to vaporize. The company, ONEOK Inc., insisted the air levels posed no risk to the public. Shortly before 5 p.m., none of the 1,000 residents of Medford, located near the Kansas border and about 2.5 miles north of the plant, had checked into a shelter set up in

nearby Wakita. The leak shut down U.S. 81, the major highway in the area. An Oklahoma Department of Transportation spokesman said the highway would not reopen before March 2.
Source: http://www.washingtonpost.com/national/officials-urge-evacuation-of-okla-town-as-propane-leak-at-fuel-storage-plant-enters-3rd-day/2012/03/01/gIQAjQJQlR_story.html

3. *March 1, Durango Herald* – (New Mexico) **Federal court rules against power generator.** A federal court told the Public Service Co. of New Mexico (PNW) March 1 it must install equipment to reduce significantly the 16,000 tons a year of haze and ozone and nitrogen pollution produced by the smokestacks at the San Juan Generating Station near Farmington, New Mexico. The San Juan Generating Station is located just outside Navajo tribal land near Farmington. The federal court ruling comes shortly after a report that said while PNM was battling the EPA order, it had raised residential power rates 41 percent since 2008. Nitrogen pollution from power plants has been a major source of harmful haze in the Four Corners for decades.
Source: http://durangoherald.com/article/20120302/NEWS01/703029911/-1/s

4. *March 1, Alaska Dispatch* – (Alaska) **Fire at BP facility slows Alaska oil production.** A small fire at a Prudhoe Bay gathering center run by BP in Alaska, led to a shutdown February 29, an official said. A spokeswoman with the Alaska Oil and Gas Conservation Commission said there were no injuries or explosions at Gathering Center 2. The center separates about 77,000 barrels of oil daily from natural gas and water. It is one of about a dozen plants that process oil before it is shipped down the trans-Alaska pipeline, a BP spokesman said. Employees "observed a flame and heard a noise at one of two low-pressure gas-handling" buildings, he said in an e-mail. There were no injuries, explosions or spilled oil. The fire did cause a drop in production, but the conservation commission spokeswoman did not know the exact amount lost.
Source: http://www.alaskadispatch.com/article/fire-bp-facility-slows-alaska-oil-production

For more stories, see items **55** and **62**

[Return to top]

Chemical Industry Sector

5. *March 2, Associated Press* – (California) **Work safety fines proposed for researcher death.** A northern California technology firm faces nearly $56,000 in workplace safety fines for a deadly explosion last year. A scientist was mixing methane, helium, and nitrogen when a gas cylinder exploded last September at Menlo Park's Membrane Technology & Research. He was killed and another researcher was hurt. The San Jose Mercury News said a California Occupational Safety and Health Administration (Cal/OSHA) report released March 1 said pressures in the cylinder exceeded allowable amounts, and the cylinder was not equipped with a proper pressure relief valve. Cal/OSHA said the device was set to activate above 3,360 pounds per square inch, more than 10 times the maximum. Membrane was notified February 24 that it faced six

serious and one general violation.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/03/02/state/n054739S80.DTL

6. *March 2, Bloomberg* – (International) **Former DuPont worker pleads guilty in economic espionage case.** A former DuPont Co. employee pleaded guilty March 1 in federal court in San Francisco to conspiring to steal trade secrets about titanium dioxide technology and provide them to China's state-owned Pangang Group Co. The naturalized U.S. citizen who spent 35 years at DuPont said he used the firm's trade secrets to help Pangang, which was building a 100,000 metric-ton-per-year plant to produce titanium dioxide, a white pigment used in paints, plastics, and paper. He admitted to one count of conspiracy to commit economic espionage. The convict is cooperating with the government in an investigation of DuPont trade secret theft, according to his plea agreement. He was with DuPont from 1966 to 2002 and while there worked on chloride-route titanium oxide processing, prosecutors said in court filings. A Pangang Group California businessman, his wife, and another former DuPont employee also face charges. The maximum sentence for conspiracy to commit economic espionage is 15 years in prison, a $500,000 fine, and restitution as ordered by a judge.
Source: http://www.bloomberg.com/news/2012-03-02/former-dupont-worker-pleads-guilty-in-trade-secrets-case.html

7. *March 1, U.S. Environmental Protection Agency* – (Oregon) **EPA ensures Oregon distributor properly labels pesticides.** Wilbur-Ellis Company, an international distributor of agricultural products located in Hood River, Oregon, violated federal pesticide laws by repeatedly omitting important manufacturing information on product labels, according to a settlement with the U.S. Environmental Protection Agency (EPA) announced March 1. The settlement follows a 2010 Oregon Department of Agriculture inspection. Inspectors found Wilbur-Ellis sold and distributed mislabeled "Supreme Oil," an insecticidal spray, 37 times. The EPA issued a Stop-Sale Order and helped bring the company into compliance. Wilbur-Ellis has had similar violations of the Insecticide, Fungicide, and Rodenticide Act in the past. The company has agreed to pay a $50,320 fine for the violations, and has committed to revising its labeling practices. Supreme Oil is a plant-based insecticidal spray that controls a variety of insect pests on fruits and vegetables.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/93361cf9304b7c83852579b400630ecb?OpenDocument

For more stories, see items **30** and **32**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *March 1, Reuters* – (National) **US NRC to propose first post-Fukushima safety rules.** U.S. nuclear regulators moved to issue new rules to deal with safety issues raised

by the Fukushima nuclear accident, Reuters reported March 1. Three members of the Nuclear Regulatory Commission (NRC) voted to issue the first of three proposed rules recommended by the agency staff, although the commissioners differed on some details. The staff said its recommendations, based on eight changes identified by the NRC's Fukushima task force, could move forward without significant delay, with implementation by the end of 2016.
Source: http://www.reuters.com/article/2012/03/01/utilities-nrc-fukushima-idUSL2E8E1GTQ20120301

[Return to top]

Critical Manufacturing Sector

9. *March 2, U.S. Department of Transportation* – (National) **NHTSA recall notice - Volvo S60, S80, XC60, XC70 seat wire harnesses.** Volvo announced March 2 the recall of 17,000 model year 2012 S60, S80, XC60, and XC70 vehicles manufactured from May 16, 2011 through October 6, 2011. The wire harness under the front seats may have not been attached properly to the seat frame. As a result, when the seats are moved to adjust the seating position, the wire harness may get pulled, causing it to disconnect. In the event of a crash, the front and/or side impact air bags may deploy improperly or not at all, increasing the risk of injury. Also, the lap belt pretensioner may not deploy. Volvo will notify owners, and dealers will inspect and, if necessary, secure the seat wire harness. The safety recall is expected to begin March 30.
Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V075000&summary=true&prod_id=1181768&PrintVersion=YES

[Return to top]

Defense Industrial Base Sector

10. *March 1, Defense News* – (California) **LCS Freedom back in dry dock.** Barely a month after leaving dockyard, the Littoral Combat Ships (LCS) Freedom, is back in dry dock in San Diego, this time to fix a broken shaft seal that caused minor flooding on board the ship a month ago. "The Freedom is undergoing a 6-week drydocking availability to repair the damaged inboard port shaft mechanical seal," a spokeswoman for the Naval Surface Forces command in San Diego, said March 1. While in dry dock, engineers from the Naval Sea Systems Command and Lockheed Martin, prime contractor for the LCS 1-class, will pull the propeller shaft and examine it and its seals to determine why and how the newly installed seal broke. The flooding took place February 1 while the ship was under way off southern California on post-overhaul sea trials. All four of the ship's shafts were removed for examination during that overhaul, then reinstalled with new seals. The trials were to test the work, which began in the fall of 2011. "Minor flooding" took place in the ship's shaft alley and bilges before an inflatable boot seal was deployed to contain the flooding, the spokeswoman said. The ship returned to San Diego under her own power.

Source: http://www.defensenews.com/article/20120301/DEFREG02/303010014/LCS-Freedom-Back-Dry-Dock?odyssey=tab|topnews|text|FRONTPAGE

11. *March 1, Lompoc Record* – (California) **Planned missile test postponed.** A Minuteman 3 test planned for March 1 from Vandenberg Air Force Base in California was postponed so crews could swap out a possibly problematic part, officials said. "The test launch is delayed in order to replace a test-unique tracking component used only on test missiles," Air Force Global Strike Command officials said. "The test-unique tracking component monitors missile location within geographic boundaries of the test range." A new launch date has not been set yet, officials said. The test was scheduled to occur between 2:01 a.m. and 8:01 a.m. from an underground silo. However, February 27, officials at Air Force Global Strike Command decided to delay the launch, citing a review of data from a Minuteman 3 test February 25. That unarmed Minuteman missile launched successfully at 2:46 a.m., Global Strike Command officials said of the mission dubbed Glory Trip-203. "Based on system performance analysis during GT-203 and an assessment of like components in the inventory, engineers have determined there is a potential for loss of signal continuity in one of the redundant tracking systems," they said. "We do not know for sure if there is a problem with the test missile originally scheduled to launch ...; however, engineers have recommended that the component in question be replaced." Replacing the part should take 3 to 4 days, officials added.
Source: http://www.lompocrecord.com/news/local/military/vandenberg/planned-missile-test-postponed/article_13492e9a-6367-11e1-a651-0019bb2963f4.html

12. *February 29, Military Times* – (International) **2 SUVs with secret gear stolen from Kabul base.** Two U.S. Army vehicles equipped with highly classified technology used to jam roadside bombs were stolen from soldiers on a military base in Afghanistan, Military Times reported February 29. The vehicles — both black up-armored Toyota Land Cruisers outfitted with CREW Duke electronic jamming systems — vanished in January from Camp Eggers in Kabul, according to a notice on Army Criminal Investigation Command's Web site. The vehicles would be "priceless" to an enemy, who might attempt to reverse-engineer the jammer or use the vehicles to launch a trojan horse-style attack, said a former official with the national security division of the Defense Investigative Service.
Source: http://www.militarytimes.com/news/2012/02/army-2-suvs-with-secret-gear-stolen-from-kabul-base-022912/

For another story, see item **52**

[Return to top]

Banking and Finance Sector

13. *March 2, Help Net Security* – (National) **Bogus US SEC notification leads to malware.** Notifications purportedly sent by the U.S. Securities and Exchange Commission have been hitting in-boxes and trying to trick users into following a malicious link, GFI warned March 2. Those who open the link included in the e-mail

will be redirected through a number of sites and will finally end at one that hosts the Blackhole exploit kit, which is able to take advantage of many Adobe Reader, Acrobat and Flash vulnerabilities, as well as some in Java and Windows Media Player. If the kit manages to exploit one of those, the user is taken to a Web site where he can download the about.exe file. This is not a document containing details of the complaint, but a variant of the Zeus/Zbot information-stealing trojan that is currently detected only by a dozen of the AV solutions employed by VirusTotal.
Source: http://www.net-security.org/malware_news.php?id=2022

14. *March 2, The Lower Westchester Loop* – (New York) **Over $150k skimmed from Larchmont Citibank, victims to be repaid.** Larchmont, New York police now say six individuals have reported unauthorized withdrawals from their bank accounts –- one of whom lost a total of $130,000, the Lower Westchester Loop reported March 2. The other victims reported losses of thousands of dollars. Citibank sent this response to the ATM skimming that occurred at its Larchmont branch: "Citibank identified illegal skimming devices placed on our ATM location at 1920 Palmer Ave. and took corrective action to prevent this type of skimming fraud."
Source: http://theloopny.com/blog/over-150k-skimmed-from-larchmont-citibank-victims-to-be-repaid/

15. *March 2, Ars Technica* – (International) **Bitcoins worth $228,000 stolen from customers of hacked Webhost.** Online bandits made off with at least $228,000 worth of the virtual currency known as Bitcoin after exploiting a vulnerability in a widely used Web host that gave unfettered access to eight victims' digital wallets, Ars Technica reported March 2. Ars Technica was able to confirm the theft of 46,703 BTC (Bitcoins), worth about $228,845 in U.S. currency. More than 43,000 of the stolen BTC belonged to a Bitcoin trading platform known as Bitcoinica, the company's chief executive and lead developer, told Ars Technica. Another 3,094 BTC were lifted from the virtual purse of a freelance programmer from the Czech Republic. He said in an interview that a separate Bitcoin user he has been in contact with lost 50 BTC to the same attackers. The lead Bitcoin programmer told Ars Technica he lost all 5 BTC he had stored in one online account. Hours after the two programmers brought the March 1 attacks to light, cloud services provider Linode confirmed a hacker targeted Bitcoin wallets stored on its servers after compromising a customer service portal. "All activity by the intruder was limited to a total of eight customers, all of which had references to 'bitcoin,' " Linode's advisory stated. "The intruder proceeded to compromise those Linode Manager accounts, with the apparent goal of finding and transferring any bitcoins. Those customers affected have been notified."
Source: http://arstechnica.com/business/news/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost.ars

16. *March 2, The Register* – (International) **Anonymous Web weapon backfires with hidden banking Trojan.** Anonymous supporters queuing up to participate in denial-of-service attacks are being tricked into installing ZeuS botnet clients. Hacktivists grabbed what they thought was the Slowloris tool, which is designed to flood Web sites with open connections and ultimately knock them offline. However, the download included a strain of ZeuS, which promptly installed itself on their Microsoft Windows machines.

The trojan will carry out the distributed attacks, but that's not all it does — it will also steal users' online banking credentials, Web mail logins, and cookies. The deception began January 20, Symantec reported. Malware peddlers swiped the template of an Anonymous guide to launching denial-of-service attacks from Pastebin, modified it to include a link to Slowloris, and reposted the message on Pastebin to snare victims.
Source:
http://www.theregister.co.uk/2012/03/02/trojan_attack_tool_targets_hacktivists/

17. *March 2, U.S. Securities and Exchange Commission* – (National) **Judge orders Brookstreet CEO to pay $10 million penalty in SEC case.** The U.S. Securities and Exchange Commission (SEC) announced March 2 that a federal judge has ordered the former chief executive officer (CEO) of Brookstreet Securities Corp. to pay a maximum $10 million penalty in a securities fraud case related to the financial crisis. The SEC litigated the case beginning in December 2009, when the agency charged the CEO and Brookstreet with fraud for systematically selling risky mortgage-backed securities to customers with conservative investment goals. Brookstreet and its CEO developed a program through which the firm's registered representatives sold particularly risky and illiquid types of Collateralized Mortgage Obligations (CMOs) to more than 1,000 seniors, retirees, and others for whom the securities were unsuitable. Brookstreet and its CEO continued to promote and sell the risky CMOs even after the CEO received numerous warnings these were dangerous investments that could become worthless overnight. The fraud caused severe investor losses and eventually caused the firm to collapse.
Source: http://www.sec.gov/news/press/2012/2012-37.htm

18. *March 1, USA Today* – (International) **Phishing scam targets taxpayers who use tax software.** The growing popularity of tax preparation software has led to a rise in e-mail scams targeted at do-it-yourself taxpayers, USA Today reported March 1. Intuit, parent of TurboTax and numerous other tax preparation products, has seen a "marked increase" this year in reports of fraudulent e-mails that claim to come from it, a spokeswoman said. Recent examples included one with "Your Intuit.com order confirmation" in the subject line. Another read: "QuickBooks Security Notice." In addition to stealing financial data, some of these e-mails contain fake Web links that could download viruses. Identity thieves target tax software providers for two reasons: volume and confusion. Spammers who send mass e-mails have a good chance of hitting many tax software users. More than 24 million taxpayers used TurboTax last year; more than 50 million purchased some kind of Intuit product, the Intuit spokeswoman said. TurboTax, H&R Block and other software providers also routinely send customers e-mails advising them of the status of their tax returns. For that reason, customers often feel they cannot afford to ignore what appears to be an e-mail from their software provider, the spokeswoman said.
Source: http://www.usatoday.com/money/perfi/taxes/story/2012-03-01/tax-phishing-scam/53323296/1

19. *March 1, Baltimore Sun* – (Maryland) **Glen Arm home builder arrested in $14M investment fraud.** A Glen Arm, Maryland home builder was indicted March 1 in connection with a $14 million investment fraud, prosecutors said. A federal grand jury

indicted the man for conspiring to commit wire fraud, Maryland's U.S. attorney's office announced. The builder, as well as a co-conspirator, told investors that in order to obtain loans for commercial real estate projects, he needed an escrow account with "large sums of money" that showed the business had "liquidity," according to a statement from the U.S. attorney's office. Investors, assured by an agreement that said no one could touch their funds without their authorization, gave the man the money to put into the account, the statement said. For at least 2 years, from August 2009 to August 2011, the man and his colleague withdrew millions from the escrow account and used it to pay off personal and business debts, according to federal prosecutors. They hid their fraud by sending out fake bank statements, and paid money owed to early investors with funds invested later on, according to the statement. If convicted, he faces to up to 20 years in prison.
Source: http://www.baltimoresun.com/news/maryland/bs-md-homebuilder-indictment-20120301,0,3679365.story

20. *March 1, Associated Press* – (Tennessee) **2 Georgia men accused of using counterfeit ATM cards in Tennessee to steal about $72,000.** A federal grand jury in Chattanooga, Tennessee, has indicted two Georgia men on charges they used counterfeit ATM cards to steal about $72,000 from bank customers, the Associated Press reported March 1. According to the U.S. attorney's office, the two man are accused of using the false ATM cards, bank fraud, and aggravated identity theft. Prosecutors said the two used a skimmer to obtain bank account numbers and PIN numbers of Regions Bank customers in September and October 2011 in East Ridge, Tennessee. Investigators said the two were found with 39 counterfeit ATM cards last October.
Source:
http://www.therepublic.com/view/story/4bc24ab8a18e4ac7bb416f10aa42514a/TN--ATM-Cards-Fraud/

21. *March 1, Associated Press* – (California) **Southern California bank hostage rescued.** SWAT officers in Buena Park, California, rescued a bank manager held at gunpoint by a would-be robber who was arrested March 1 after being wounded in a shootout with police. The female manager was safe after police shot the middle-aged suspect as he went to the front of the Saehan Bank with the female banker at gunpoint, the Buena Park police chief said. Video from a television helicopter showed at least eight officers with guns drawn approaching the bank in a small strip mall when the front window shattered and the woman was pulled from inside the shattered door. Three officers suffered minor wounds to their arms, but it was not immediately known how they received their injuries or whether the gunman returned fire. The gunman, who has not been identified, was in custody and listed in serious condition. He entered the bank shortly after 11 a.m. and seven people inside were released, authorities said. The police chief characterized the incident as a botched robbery and said the man, armed possibly with a shotgun, had made demands during the 4-hour standoff. "He was coming out the door to retrieve something he demanded" when the shooting occurred, the chief said.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/03/01/state/n124358S28.DTL&type=business

[Return to top]

Transportation Sector

22. *March 2, Associated Press* – (Minnesota) **Barge sinks in Duluth harbor.** Workers are trying to recover a 1,000-gallon propane tank from a barge that sank in the Duluth harbor in Duluth, Minnesota, the Associated Press reported March 2. The U.S. Coast Guard (USCG) was working with salvage companies to get the nearly full tank off the sunken 120-foot-long barge, which sank in a harbor slip. The USCG said it does not know why the barge went down. The 106 year-old barge is owned by Duluth Timber Co. and will have to be removed if it is a navigation hazard or causes pollution.
Source: http://www.news8000.com/news/Barge-sinks-in-Duluth-harbor/-/326/9199058/-/15aqmgkz/-/

23. *March 2, Sarasota Herald-Tribune* – (Florida) **I-75 opened after fog forces early closure.** All lanes of Interstate 75 were reopened to traffic after heavy fog forced authorities to close a 10-mile stretch of the highway in southern Sarasota County, Florida, March 2. There were no reports of accidents or incidents related to the foggy conditions, troopers said. The closure led to lengthy traffic delays on several neighboring highways. Forecasts called for heavy fog to roll into the area again March 2 or 3, according to the National Weather Service.
Source:
http://www.heraldtribune.com/article/20120302/BREAKING/120309939/2055/NEWS?p=1&tc=pg

24. *March 2, CBS News* – (Pennsylvania) **Man faces DUI charges after driving Jeep onto Philadelphia Airport runway.** Police said an intoxicated man in an SUV crashed through a security gate and drove onto two runways at Philadelphia International Airport March 1. Investigators said the incident began when a Jeep Cherokee crashed through a chain-link fence surrounding the airport. The high-speed chase down the runway was captured by ground radar and controllers. The man drove around the airport for several minutes before police were able to stop the car and take him into custody. He was taken to a local hospital for a psychiatric evaluation and now faces DUI charges. Federal charges are also possible. Authorities believe this is an isolated incident with no link to terrorism. The airport was shutdown for about 30 minutes as police investigated. When it reopened, incoming flights were delayed for a short time.
Source: http://www.cbsnews.com/8301-504083_162-57389248-504083/man-faces-dui-charges-after-driving-jeep-onto-philadelphia-airport-runway/

25. *March 1, Associated Press* – (International) **Alarm, lifevests and lifeboats: Cruise ship docks.** The Costa Allegra docked in the Seychelles March 1 nearly 3 full days after a fire broke out in the ship's generator room, leaving passengers without working toilets, running water, or air conditioning in a region of the Indian Ocean pirates are known to prowl. Cabin temperatures were estimated to have been 100 to 110 degrees Fahrenheit, forcing passengers to sleep on deck chairs. The fire came only 6 weeks after the Costa Concordia capsized off Italy, killing 25 people and leaving 7 missing. After the generator on the Allegra caught fire February 27, a ship captain sounded the

general alarm. Passengers could not see the fire, but they could smell it and see smoke. Crew members extinguished the blaze within an hour, but the alarm was kept in place 2 hours more. A passenger said the response was disorganized. There was chaos for 3 or 4 hours. The waters off East Africa are Somali pirate territory. The attacks crippled the Seychelles tourism industry after wary cruise companies stopped coming in 2009.
Source: http://abcnews.go.com/International/wireStory/disabled-cruise-ship-arrives-seychelles-port-15822311#.T1D3tHnW58E

For more stories, see items **2** and **56**

[Return to top]

Postal and Shipping Sector

26. *March 2, Associated Press* – (Wisconsin) **Guilty plea in theft of 9,000 pieces of mail.** A former Coulee Region postal worker pleaded guilty in federal court to stealing 9,000 pieces of mail in La Crosse, Wisconsin. He told a federal judge in Madison March 1 that he took the mail because "times were tough, money was tight and bills were piling up." A man who mailed cards containing $2 bills to his grandchildren alerted authorities after the cards were delivered, but had been opened and were missing the bills. The La Crosse Tribune reported the postal worker admitted in court to taking money from envelopes he opened. The stolen mail was held as evidence but will now be released for delivery.
Source: http://www.chicagotribune.com/news/chi-ap-wi-postaltheft,0,3842604.story

27. *March 1, Minneapolis Star-Tribune* – (Minnesota) **Postage scam nets Prior Lake man 18 months in prison.** A Prior Lake, Minnesota man who found it funny that it was so easy to make phony postage meter stamps was sentenced to 18 months in prison and ordered to pay nearly a quarter of a million dollars in restitution. The man was sentenced February 29 in federal court in Saint Paul, Minnesota, after pleading guilty to counterfeiting the stamps thousands of times. According to the plea agreement, the man said he created the counterfeit stamps using his personal computer and printer, and using copies of postage meter stamps he bought online. The man will repay $230,000 to the U.S. Postal Service.
Source: http://www.startribune.com/local/south/141044153.html

[Return to top]

Agriculture and Food Sector

28. *March 2, NewsCore* – (National; International) **3 more orange juice imports positive for fungicide, FDA says.** March 1, the U.S. Food and Drug Administration (FDA) said 3 additional shipments of imported orange juice tested positive for a fungicide not approved for use on oranges in the United States, bringing the total number of detained or refused shipments to 27. Of the three most recent samples found positive for the fungicide carbendazim, two were from Brazil and one was from the Dominican Republic. Of the other 24 shipments, 12 came from Brazil and 12 from Canada. Since

the FDA began to sample imports January 4, a total of 106 shipments have been tested, of which 78 came back negative and 63 were released for U.S. consumption. The remaining shipments are pending U.S. government approval over issues unrelated to the fungicide. FDA officials said they began testing all orange juice imports shortly after Coca-Cola Co. reported finding the fungicide in juice it imported from Brazil. Carbendazim is considered safe for dozens of other crops sold in the United States, including apples, cherries, and bananas.
Source: http://www.foxnews.com/health/2012/03/02/3-more-orange-juice-imports-positive-for-fungicide-fda-says/

29. *March 1, KEZI 9 Eugene* – (Oregon) **County conducts norovirus investigation at Eugene restaurant.** Lane County Health & Human Services wrapped up an investigation into a reported norovirus outbreak at Olive Garden in Eugene, Oregon, KEZI 9 Eugene reported March 1. Over 2 weeks ago, a handful of people called the health department to say they believed they got sick after eating at the Olive Garden. Because the calls came from two separate groups, the health department investigated. Samples were taken from three of the people who ate at the restaurant. A number of samples were also collected from employees. At least one of the samples came back positive, but the health department would not say which group it came from — customers or employees. It said Olive Garden cooperated. "They spent two days cleaning top to bottom," an environmental health specialist said. The health department said results of the investigation are inconclusive as to whether the virus came from the restaurant.
Source: http://kezi.com/news/local/240381

30. *March 1, CNET News* – (International) **AntiSec dumps Monsanto data on the Web.** Anonymous continued its ongoing attack on agricultural biotech giant Monsanto March 1 by publishing an outdated database of the company's material. That was the newest in a barrage of strikes from hackers aligned with Anonymous who operate under the "AntiSec" banner. In a statement posted with the database on Pastebin, the hacktivist group wrote it was aware exposing the database would not do much harm to Monsanto, but warned it would continue to target the company. "Your continued attack on the world's food supply, as well as the health of those who eat it, has earned you our full attention," wrote AntiSec. Anonymous' battle with Monsanto began in July 2011 when the hackers disrupted the company's Web site and then released data on about 2,500 individuals involved in the agriculture industry. According to Monsanto, 10 percent of this information was related to current and former Monsanto employees. Monsanto was one of seven companies that supplied the U.S. military with Agent Orange during the Vietnam War and, for a while, made bovine growth hormones. Now it focuses on making genetically engineered seeds and pesticides. AntiSec said the reason for the attacks is to protest the company's lawsuits against organic dairy farmers for stating on labels that their products do not contain growth hormones.
Source: http://news.cnet.com/8301-1009_3-57389119-83/antisec-dumps-monsanto-data-on-the-web/

For more stories, see items **1**, **7**, and **32**

[Return to top]

Water Sector

31. *March 2, WBKN 27 Youngstown* – (Ohio) **Cause of Struthers plant explosion still unknown.** Two men injured in an explosion March 1 at the Struthers wastewater treatment plant in Ohio were listed in critical condition as of March 2. The men were air lifted to a Pittsburgh hospital following the explosion. Both suffered extensive burns. The explosion happened in a compression room that is used in the treatment of sludge coming into the plant. State and federal investigators were trying to pinpoint what caused some sort of gas to build up and then ignite with so much force. The Struthers fire chief said that section of the plant remains closed but that the rest of the facility was in operation. Investigators from the state fire marshal's office and Occupational Safety and Health Administration were investigating the cause.
Source: http://www.wkbn.com/mostpopular/story/Update-Victims-in-Sewage-Plant-Explosion-Listed/xu8rvpK9a022B3tLwaH93g.cspx

32. *March 1, U.S. Environmental Protection Agency* – (West Virginia) **Welch, W.Va. settles Clean Water Act violations.** The U.S. Environmental Protection Agency and West Virginia announced March 1 they have settled violations of the Clean Water Act involving sewage overflows in Welch, West Virginia. Under the settlement filed by the U.S. Justice Department in federal district court, the city agreed to implement a long term control plan to eliminate combined sewer overflows (CSOs) at an estimated cost of $16 to $23 million. Welch will completely separate its sanitary wastewater and storm sewers and will implement a plan for upgrading its treatment plant and monitoring system. Once implemented, the steps that Welch is required to take under this agreement will eliminate CSOs resulting in the discharge of about 400,000 gallons of raw sewage annually. Welch will also pay a $5,000 penalty for past violations, split between the United States and West Virginia.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/adc360174adcb6ff852579b40072d555!OpenDocument

33. *March 1, Buffalo News* – (New York) **$20,000 fire damages at Island treatment plant.** Improperly stored oily rags caused a fire March 1 in an auxiliary building at the Grand Island, New York wastewater treatment plant. The fire was put out by crews from the Grand Island Fire Company in less than a half-hour. Damage was listed as $15,000 to the structure and $5,000 to contents, fire officials said.
Source: http://www.buffalonews.com/city/communities/grand-island/article746046.ece

34. *March 1, ExploreHoward.com* – (Maryland) **100,000 gallons of sewage spills into Little Patuxent.** A malfunction at a Howard County, Maryland water treatment plant February 28 dumped about 100,000 gallons of sewage into Guilford Run and the Little Patuxent River, the county health department said. Software problems caused the sewage — which health officials said had been 90 percent treated — to be released from the Little Patuxent Water Reclamation Plant. The facility handles wastewater from Columbia, North Laurel, and Savage, according to the county public works

department. Health officials said they expected the sewage would quickly be diluted due to it largely having been treated and because of heavy rain the following day. The health department warned the public to avoid contact with the affected areas. County officials were working with the software vendor to prevent another malfunction.
Source: http://www.baltimoresun.com/explore/howard/news/ph-ho-cf-glances-sewage-spill-0308-20120301,0,4939068.story

For more stories, see items **1** and **62**

[Return to top]

Public Health and Healthcare Sector

35. *March 2, Associated Press* – (California) **Calif. doc charged with murder for prescriptions.** A Los Angeles, Calofinia doctor, whom authorities have dubbed "Dr. Feelgood," passed out prescriptions for drugs like Xanax, OxyContin, Vicodin, and Adderall at a rate of 25 per day for 3 years, with only cursory patient examinations and a minimum of questions, authorities said. And after a long probe involving U.S. Drug Enforcement Agency (DEA) agents posing as patients, Dr. Feelgood was charged in the deaths of three otherwise healthy men in their 20s. She is also charged with 21 other felony counts alleging she prescribed drugs using fraud and without a legitimate purpose. Dr. Feelgood and her husband, also a doctor, opened a storefront medical office in 2005 in the Los Angeles suburb of Rowland Heights. She came under scrutiny by the California Medical Board and the DEA in 2008 after a pharmacy reported problems with her prescriptions. She wrote more than 27,000 prescriptions over a 3-year period starting in January 2007, according to a DEA affidavit. The DEA suspended her license to write prescriptions in 2010, and the Osteopathic Medical Board of California said Dr. Feelgood voluntarily surrendered her medical license. Her husband continues to run their clinic.
Source: http://www.chron.com/news/article/CA-doc-faces-rare-murder-charges-for-prescriptions-3376405.php

36. *March 2, San Luis Obispo Tribune* – (California) **Atascadero State Hospital fined for safety violations.** California safety investigators March 1 issued three citations totaling $38,555 against Atascadero State Hospital (ASH) for unsafe working conditions for staff treating the facility's mentally ill and violent offenders. The California Division of Occupational Safety and Health issued its findings after conducting an investigation late last year that included a walk-through. The investigation was prompted by employee complaints, according to the president of the California Association of Psychiatric Technicians' ASH chapter. The violation with the largest proposed fine — $25,000 — claims that from 1994 to 2011 ASH failed to correct workplace safety hazards that led to patient assaults on employees. The report cites that an average of eight staff assaults occurred per month from January 2007 to October 2011, resulting in many injuries. ASH was also faulted for not effectively implementing certain safety features. The concerns include lax control of patient access, inadequate alarms, a lack of security personnel, and inadequate staffing. ASH was also faulted for not properly protecting the confidentiality of employees' names on state forms, and for not giving

employees the proper protective gear for touching blood or for when working with agitated patients.
Source: http://www.sanluisobispo.com/2012/03/01/1971416/atascadero-state-hospital-osha.html

37. *March 1, New London Day* – (Connecticut) **PharmaLive: Eight arrested during protest at Pfizer plant.** Eight people from the Groton, Connecticut Occupy movement were arrested February 29 outside the main gate of Pfizer Inc. when they allegedly crossed police lines and refused to leave the company's Eastern Point Road property. Seven of the protesters linked arms just outside the entrance and refused to move, telling a Pfizer contractor they wanted to talk to a company official. One other protester was arrested for crossing police lines. By early afternoon, the protesters had dispersed to conduct teach-ins at a nearby church. Organizers opted against a protest in the Fort Trumbull neighborhood in New London, where a controversial eminent-domain effort dislodged a neighborhood partly at Pfizer's behest, because they wanted to focus on what they see as illicit attempts by firms to pass legislation with little public input. The full contingent numbered nearly 100 protesters, who marched around Pfizer's largest worldwide research site for most of the morning. The protest involved more than 90 cities nationwide.
Source: http://pharmalive.com/News/index.cfm?articleid=828477

38. *March 1, Pennsylvania Patient Safety Authority* – (Pennsylvania) **Pennsylvania hospital data shows increased likelihood of medication errors when in-house pharmacy is closed.** Between June 2004 and September 2010 Pennsylvania hospitals submitted 519 medication error reports to the Patient Safety Authority that implied an event occurred while the pharmacy department was closed, according to information published in the March Pennsylvania Patient Safety Advisory released March 1. The most common types of medication errors reported by facilities when the pharmacy was closed include wrong-drug events (30.4 percent), drug omissions (28.9 percent) and prescription or refill delays (11 percent). According to the data, the incorrect drug was retrieved from an automated dispensing cabinet or night cabinet in 82 percent of 130 wrong-drug events. A senior patient safety analyst for the Pennsylvania Patent Safety Authority said that of the top 10 medications involved in the events, four were high-alert medications, or drugs that have an increased risk of causing significant patient harm when used in error. He said on-site 24-hour pharmaceutical services can provide a more secure drug storage and distribution system. It also reduces the need for night cabinets, non-pharmacist access to the pharmacy, and access to medications stored in automated dispensing cabinets without prior order review by a pharmacist.
Source: http://www.sacbee.com/2012/03/01/4303459/pennsylvania-hospital-data-shows.html

39. *March 1, Legal Newsline* – (New York) **Drug companies settling multistate claims.** The New York Attorney General announced settlements totaling $28 million February 28 with two pharmaceutical companies that allegedly violated Medicaid regulations. As part of two multistate agreements, Dava Pharmaceuticals Inc. and KV Pharmaceutical Co. will pay the state of New York for alleged separate violations of the False Claims Act. Dava allegedly misclassified drugs to evade paying obligations to

Medicaid. KV allegedly failed to advise the Centers for Medicare and Medicaid Services about two drugs that did not qualify for coverage under state and federal health care programs. The state of New York will receive more than $2.5 million as its portion of the settlements.
Source: http://www.legalnewsline.com/news/235367-drug-companies-settling-multistate-claims

40. *February 29, Bloomberg News* – (National) **McAfee hacker says Medtronic insulin pumps vulnerable to attack.** Some Medtronic Inc. insulin pumps are vulnerable to a hacking attack that could let someone break into the devices from hundreds of feet away, disable security alarms, and dump insulin directly into diabetics' bloodstreams, according to a computer-security researcher at McAfee Inc. The McAfee researcher said he can remotely control several types of Medtronic pumps. After first discussing the vulnerability last year at a small hacker conference in Florida, he has discovered more ways to exploit the weakness, including overriding security features such as vibration warnings. He is trying to increase awareness of the risks of medical devices. Medtronic has responded to the risks by hiring security teams from three organizations to inspect its products. Medical-device security first became a flash point last year when a diabetic patient in Idaho showed hackers could manipulate the best-selling brand of pump he used. He got the attention of lawmakers, who pressed the Government Accountability Office to investigate whether the industry's cybersecurity rules are tough enough. The report from that probe is due in July.
Source: http://www.bloomberg.com/news/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack.html

For another story, see item **56**

[Return to top]

Government Facilities Sector

41. *March 2, Associated Press* – (Arizona) **Student hurt, man jailed in Ariz. school shooting.** Authorities worked to determine what motivated a man to allegedly fire a rifle indiscriminately at a Willcox, Arizona high school, injuring a student who was watching a baseball game. The student suffered minor cuts from flying glass when the car he was in was shot at March 1, authorities said. The man was arrested shortly after the shooting at Willcox High School, and the weapon he was accused of using was recovered about a block from the scene, according to the Willcox Department of Public Safety (DPS). The DPS chief said authorities believe he fired three rounds.
Source: http://www.chron.com/news/article/Student-hurt-man-jailed-in-Ariz-school-shooting-3375159.php

42. *March 2, CNN* – (Ohio) **Ohio high schoolers head back to class after fatal shooting.** Students at Ohio's Chardon High School headed back to class March 2 for the first time since a gunman walked into the school's cafeteria and killed three teenagers. The person who authorities said is responsible for the February 27 attack was charged March 1 with three counts of aggravated murder, two counts of attempted

aggravated murder, and one of felonious assault, the latter related to an individual who was "nicked in the ear" by a bullet, according to the Geauga County prosecuting attorney.
Source: http://schoolsofthought.blogs.cnn.com/2012/03/02/ohio-high-schoolers-head-back-to-class-after-fatal-shooting/

43. *March 1, Government Computer News* – (National; International) **As deadline nears, federal agencies mostly free of DNSChanger.** Although millions of computers around the world could still contain the DNSChanger malware used by an Internet fraud ring, government agencies and large enterprises appear to have done a good job of cleaning up the infections, said a member of the DNSChanger Working Group, Government Computer News reported March 1. The member said early in February that, based on information gleaned from traffic to rogue DNS servers, it appeared that half of all Fortune 500 companies and 27 of 55 major federal agencies were infected. He reported at the RSA Conference that, as of February 23, those numbers had dropped to just 3 agencies and 94 companies. The progress is important, because the non-profit Internet Systems Consortium has been operating the name servers under a court order on behalf of the Justice Department since November 2011 to ensure infected computers whose DNS requests were being directed to the rogue servers were not cut off from the Internet. The original court order expires March 8. However, there still are a large number of computers that must be cleaned up, and it is not known how many computers are infected within each agency or company. "It's hard to know exactly how many machines," he said. "It's probably millions." However, from traffic volumes, the number appears small at government agencies.
Source: http://gcn.com/articles/2012/03/01/rsa-13-federal-dnschanger-cleanup.aspx

For more stories, see items **2**, **12**, **50**, **52**, **55**, and **57**

[Return to top]

Emergency Services Sector

44. *March 2, Associated Press* – (Alabama) **Bodies of 2 missing crewmembers recovered after crash of US Coast Guard helicopter in Ala. bay.** U.S. Coast Guard officials said they recovered the bodies of two of the three crewmembers who had been missing since a helicopter crashed in Mobile Bay in Alabama. Searchers recovered the remains of the two crewmembers March 1, authorities said. A fourth crewmember, was found unresponsive and later pronounced dead shortly after the February 28 crash. Active search and rescue operations for the remaining missing crewmember were suspended, and crews were conducting salvage and recovery operations March 2, the Coast Guard said. Crews searched for 36 hours, conducting about 30 search patterns that covered 1,198 nautical miles within a search area of more than 200 square-nautical miles in an effort to locate the crewmen.
Source: http://www.washingtonpost.com/national/bodies-of-2-missing-crewmembers-recovered-after-crash-of-us-coast-guard-helicopter-in-ala-bay/2012/03/02/gIQAd4eLmR_story.html

45. *February 29, CNN* – (Texas; International) **Texas 'navy' to patrol the Rio Grande.** In March, the Texas Department of Public Safety will deploy the first of a fleet of six gunboats on the Rio Grande, the river that forms the border between Texas and Mexico, WFAA 8 Dallas reported February 29. The 34-foot-long boats, each powered by 3,300-horsepower outboard engines, will have bulletproof plating and 6 machine guns apiece. The vessels will be able to operate in as little as 2 feet of water, according to the report, and will work with U.S. Customs and Border Protection to combat drug smuggling coming across the Rio Grande.
Source: http://news.blogs.cnn.com/2012/02/29/texas-navy-to-patrol-the-rio-grande/?hpt=us_c2

For more stories, see items **21** and **57**

[Return to top]

Information Technology Sector

46. *March 2, H Security* – (International) **Phishing via NFC.** At the RSA Conference 2012, McAfee's chief technology officer (CTO) and several of his colleagues demonstrated a range of different attacks on mobile devices. They demonstrated an attack on an near field communication (NFC)-enabled smartphone: the attacker simply attaches a modified NFC tag to a legitimate surface such as an advertising poster. The poster's regular NFC tag took the browser to a donations Web site, where the donor's details could be recorded. However, the modified secondary tag diverted the smartphone browser to a phishing site that pretended to be part of the charity. The CTO said such attacks have already been observed in the wild. The researcher also demonstrated how to take control of an iPad. When a victim clicks on a link in an e-mail, a PDF file is downloaded, and malware is installed without the user's knowledge via a vulnerability in the iOS code for processing PDFs. Although the attack is based on a vulnerability that has long been closed by Apple, the expert said he assumes that newer iOS versions will continue to be vulnerable via jailbreaks. Once a device becomes infected, it establishes a connection to the command and control server and transfers, for example, its location. One click on the symbol displayed in Google Maps on the attacker's system gives access to several options: to retrieve the SMS database, record the device environment using the microphone, or access the key chain. The key chain contains any passwords for applications and online services that are stored on the device.
Source: http://www.h-online.com/security/news/item/Phishing-via-NFC-1447010.html

47. *March 1, H Security* – (International) **Bug in Plesk administration software is being actively exploited.** A critical security vulnerability in the Plesk administration program is currently being actively used to compromise affected servers. Plesk is used most often by hosting providers and provides a Web front-end for administering rented servers. The vulnerability seems to be a SQL injection problem, which an attacker can exploit to gain full administrative access to a system. Linux and Windows versions of Parallels Plesk Panel 7.6.1 - 10.3.1 are affected. Parallels, the company that publishes the software, has already fixed the vulnerability in the current versions and is even

offering micro-updates whose only purpose is to fix the problem.
Source: http://www.h-online.com/security/news/item/Bug-in-Plesk-administration-software-is-being-actively-exploited-1446587.html

48. *March 1, H Security* – (International) **Report: Thousands of embedded systems on the net without protection.** At the RSA Conference 2012, a Zscaler researcher provided evidence many embedded Web servers (EWS) can be easily accessed by outsiders via the Internet. Where multi-function printers or video conferencing systems are concerned, this can cause serious data leaks: the printers store scanned, faxed, and printed files on hard disks and then disclose documents. Video conferencing hardware allows outsiders to monitor rooms remotely or listen to meetings in progress. The researcher's aim was to scan 1 million Web servers and create a catalog of all the EWS he found. After a round of testing, he entered typical character strings from the EWS Web pages into Shodan. A scan managed to examine the 1 million servers in a short time and came up with the following results: many thousands of multi-function devices, 8,000 Cisco IOS devices, and almost 10,000 VoIP systems and phones did not require any log-in authentication. The majority of the devices were not protected by passwords. This means any Web user can access their Web interfaces through a browser and view the documents stored on such photocopiers and printers, forward incoming faxes to an external number, or record scan jobs. The scan run also identified more than 9,000 video conferencing systems by Polycom and Tandberg (now Cisco). The researcher used a video to demonstrate how he managed to monitor the targeted conference rooms via an accessible video conferencing system that provided both sound and images.
Source: http://www.h-online.com/security/news/item/Report-Thousands-of-embedded-systems-on-the-net-without-protection-1446441.html

49. *March 1, New York Times* – (International) **Et tu, Google? Android apps can also secretly copy photos.** As the New York Times reported the week of February 27, developers who make applications for Apple iOS devices have access to a user's entire photo library as long as that user allows the app to use location data. It turns out that Google, maker of the Android mobile operating system, takes it one step further. Android apps do not need permission to get a user's photos, and as long as an app has the right to go to the Internet, it can copy those photos to a remote server without any notice, according to developers and mobile security experts. It is unclear whether any apps available for Android devices are actually doing this.
Source: http://bits.blogs.nytimes.com/2012/03/01/android-photos/

50. *March 1, Computerworld* – (International) **Internet voting systems too insecure, researcher warns.** Internet voting systems are inherently insecure and should not be allowed in the upcoming general elections, a noted security researcher said at the RSA Conference 2012. The researcher, a computer scientist at Lawrence Livermore National Laboratories and chairman of the election watchdog group Verified Voting, called on election officials around the country to drop plans to allow an estimated 3.5 million voters to cast their ballots over the Internet in 2012's general elections. In an interview with Computerworld, he warned the systems that enable such voting are far too insecure to be trusted and should be jettisoned altogether. A total of 33 states allow citizens to use the Internet to cast their ballots. In a majority of cases, those eligible to

vote over the Internet receive their blank ballots over the Web, fill them in, and submit their ballots via e-mail as a PDF attachment. Some states, such as Arizona, have begun piloting projects that allow eligible voters to log in to a Web portal, authenticate themselves, and submit their ballots via the portal.
Source:
http://www.computerworld.com/s/article/9224799/Internet_voting_systems_too_insecure_researcher_warns?taxonomyId=17

51. *March 1, IDG News Service* – (International) **Republican Senators introduce their own cybersecurity bill.** Republican Senators introduced cybersecurity legislation March 1 after saying an earlier bill would create costly regulations for businesses. The sponsors of the new Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act also complained they did not have enough input on the earlier legislation. They touted the bill as a less regulatory alternative to the Cybersecurity Act, a bill introduced by two Democrats, an Independent, and a Republican in February. The Cybersecurity Act would allow the secretary of DHS to designate some private networks as critical infrastructure and require them to submit security plans to the agency. However, the SECURE IT Act has no such rules, instead focusing on encouraging private companies and the federal government to share more information about cyberthreats, sponsors said. The new bill would give legal protections to private groups that share data. The older bill also includes information-sharing provisions, but critics said legal protections would cover only businesses that share data with the U.S. government. The new bill would also increase the prison terms for many cyber crimes.
Source:
http://www.computerworld.com/s/article/9224813/Republican_senators_introduce_their_own_cybersecurity_bill?taxonomyId=17

For more stories, see items **13**, **15**, **16**, **18**, **30**, **34**, **40**, **43**, **52**, **53**, and **54**

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

52. *March 2, Reuters* – (Virginia; National) **Pentagon suffers Internet access outage.** An unspecified number of U.S. Defense Department personnel in the Washington D.C. area and in the Midwest were cut off from the public Internet for nearly 3 hours March 1 because of technical problems, a department spokeswoman said March 2. The outage was not caused by any malicious activity, said the spokeswoman, who is an Air Force lieutenant colonel. She said the networks were back up and operating at normal

capacity. The department's Defense Information Security Agency worked with commercial vendors and "mission partners" to reroute critical DoD traffic and to mitigate the issue until technical issues were resolved, she said. The number of people affected by the outage was not known, "but is estimated in the thousands, given the number of people who work in the Pentagon," the lieutenant colonel told Reuters.
Source: http://www.reuters.com/article/2012/03/02/us-cyber-pentagon-idUSTRE8211F220120302

53. *March 2, Boston Globe* – (National) **Hacker convicted of stealing Internet access.** A man was convicted March 1 in federal court in Boston on fraud charges in connection to a $1 million scheme to steal Internet access and sell products that allowed others to do the same. The jury convicted the man on seven of eight counts. Prosecutors said the man built a lucrative business between 2003 and 2009 that helped people defraud cable companies. To access Internet service, the defendant would modify, or uncap, a modem to remove filters set up by the Internet service provider, allowing the modem to have a quicker connection without the Internet service provider being able to throttle it. He would also copy other people's modem addresses, or identification codes that Internet providers use to confirm a user is a paid subscriber. According to an indictment, he was the founder and president of TCNISO Inc., a San Diego-based company whose primary business was to sell cable modem hacking software and hardware products. He and others developed hacking products that had names including Sigma, Blackcat, and DreamOS, that allowed computer users to get access to the Internet without paying for it, according to prosecutors. He also offered products that let users disguise their online identities when downloading pirated movies, records show.
Source: http://bostonglobe.com/metro/2012/03/02/man-convicted-stealing-internet-access-and-selling-secrets/9koY8vjCPxD4z5oVkRsBZO/story.html

54. *March 1, Arizona Republic* – (Arizona; California; Nevada) **Cox voice-mail service restored.** Cox Communications residential phone customers in metro Phoenix said their voice-mail service was restored March 1 following an outage that lasted at least 9 days. However, Cox officials said some customers may experience intermittent problems while technicians finalize repairs to the voice-mail system's hardware. Cox officials said March 1 that about 200,000 customers in Arizona, Southern California, and the Las Vegas area had been without the ability to leave or retrieve voice-mail messages. During the outage, customers still had the ability to make and receive phone calls. The voice-mail glitch did not affect Cox business customers, only those with residential service, the company said. Some customers were irked March 1 that in repairing the system, Cox had wiped out all saved messages, personal settings and greetings. It was the effort to save customer data that delayed the company from getting the system back online sooner following a hardware-related failure, Cox's vice president for public affairs said March 1 in an interview. Cox has more than 2 million cable-TV, Internet and telephone customers in Arizona, including an estimated 1.7 million customers in the Phoenix area.
Source:
http://www.azcentral.com/arizonarepublic/business/articles/2012/03/01/20120301cox-voice-mail-service-restored.html

For more stories, see items **46**, **48**, and **49**

[Return to top]

Commercial Facilities Sector

55. *March 2, KOLR 10 Springfield* – (Missouri) **Gas leak halted in Nixa, people being allowed back in area.** A car crash in Nixa, Missouri, March 2 caused a large natural gas leak when a vehicle struck a gas meter. The gas leak prompted an evacuation of many of the buildings in that immediate area of downtown. The gas company reported the leak under control later in the morning, but the area remained closed to traffic. The area was deemed safe by 10 a.m. Nixa Public school officials said they were required to evacuate the central office and early learning center.
Source: http://ozarksfirst.com/fulltext?nxd_id=612012

56. *March 2, Associated Press* – (South Dakota) **Fumes from cleaning chemical mix-up prompt evacuation of hotel on Sioux Falls hospital campus.** Fumes from cleaning chemicals that were accidentally mixed together prompted the evacuation of a hotel on a Sioux Falls, South Dakota hospital complex March 2. KSFY 13 Sioux Falls reported that crews blocked off the street outside the Center Inn and vented the fumes out of the building on the Avera McKennan Hospital campus. The Center Inn is a hotel for patients' families. The Argus Leader newspaper reported that one person suffered respiratory problems but recovered. A fire department battalion chief said a maintenance crew mixed bleach and acid in a laundry room.
Source:
http://www.therepublic.com/view/story/ff33f661811a4fd49ebf2e9607573243/SD--SD-Hotel-Evacuation/

57. *March 2, Associated Press* – (National) **Tornado wrecks Indiana town as Midwest is slammed with severe storms.** Powerful storms stretching from the Gulf Coast to the Great Lakes flattened buildings in several states, wrecked a small Indiana town, and bred anxiety across a wide swath of the country, the Associated Press reported March 2. Widespread damage was reported in southern Indiana, where a Clark County Sheriff's Department official said the town of Marysville is "completely gone." Dozens of houses were also damaged in Alabama and Tennessee 2 days after storms killed 13 people in the Midwest and South. Thousands of schoolchildren in several states were sent home as a precaution, and several Kentucky universities were closed. The Huntsville, Alabama mayor said students in area schools sheltered in hallways as severe weather passed. At least 20 homes were badly damaged in the Chattanooga, Tennessee area after strong winds and hail lashed the area. In the Huntsville area, five people were taken to hospitals, and several houses were leveled by what authorities believed were tornadoes. An apparent tornado also damaged a state maximum security prison about 10 miles from Huntsville, but none of the facility's approximately 2,100 inmates escaped. An Alabama Department of Corrections spokesman said the roof was damaged on two large prison dormitories that each hold about 250 men. Part of the perimeter fence was knocked down, but the prison was secure.

Source: http://www.foxnews.com/us/2012/03/02/alabama-schools-closing-early-amid-weather-threat/

58. *March 1, United Press International* – (Georgia) **Ice rink's yellow haze sickened players.** A report by the Centers for Disease Control and Prevention (CDC) said the yellow haze that hovered over an ice hockey rink in Atlanta where many were sickened was nitrogen dioxide gas, United Press International reported March 1. The report said a man was hospitalized January 4, 2011, for sudden onset of cough, shortness of breath, and hemoptysis — coughing of blood — shortly after a hockey team practice. The indoor arena had an air monitoring system for carbon monoxide and carbon dioxide, but not for nitrogen dioxide. Health investigators also found the rink's ventilation system was inoperable at the time. Thirty-one people reported symptoms consistent with nitrogen dioxide exposure. To prevent similar episodes, ice arena operators should ensure ventilation systems and alarms are operating properly and that levels of nitrogen dioxide gas and carbon monoxide are monitored continuously for early detection of increased gas levels, CDC officials advised.
Source: http://www.upi.com/Health_News/2012/03/01/Ice-rinks-yellow-haze-sickened-players/UPI-96301330660626/?spt=hs&or=hn

For more stories, see items **2**, **21**, **43**, and **51**

[Return to top]

National Monuments and Icons Sector

59. *March 2, Hendersonville Times-News* – (North Carolina) **Forest Service seeks suspects for questioning.** U.S. Forest Service law enforcement officials reopened the Bradley Creek and Turkey Pen areas of the Pisgah National Forest in North Carolina after they were closed March 1. The areas were closed to the public after authorities said two men allegedly made threats toward another group of forest visitors. Authorities were seeking the two men for questioning. In a news release, the Forest Service said the men may have been armed. Police said March 2 that the men had been found and interviewed. No arrests have been made and no charges have been filed. The investigation is continuing.
Source: http://www.blueridgenow.com/article/20120301/ARTICLES/120309955/1042/news?Title=Forest-Service-Seeks-Suspects-for-Questioning&tc=ar

60. *March 1, Joplin Globe* – (Missouri) **Fire destroys historic downtown Joplin building.** A fire of undetermined origin destroyed the historic Rains Brothers Building in Joplin, Missouri, March 1. A spokesman for the Joplin Fire Department said police dispatchers received a 9-1-1 call about the fire. Joplin firefighters arrived a few minutes afterwards. The fire produced a thick column of smoke over the downtown area as wood floors, stairwells and rooms inside the former hotel burned. Firefighters had most of the fire knocked down within an hour of the 9-1-1 call. The building, constructed in 1900, was placed on the National Register of Historic Places in 2011. The building has been vacant and in a state of disrepair for several years.

Source: http://www.joplinglobe.com/local/x1225453727/Fire-destroys-downtown-building

[Return to top]

Dams Sector

61. *March 3, Australian Broadcasting Corporation* – (International) **The Warragamba Dam is spilling.** The Warragamba Dam, Sydney, Australia's primary source of drinking water, reached full capacity and began spilling March 2, according to the Australian Braodcasting Corporation. Some 900 people in western Sydney are on stand-by for evacuation should the SES give the order. The bureau of meteorology reported a Flood Watch for moderate flooding is current for the catchment based on forecast rain for the next 2 to 3 days. A spokesman said the water was rising.
Source: http://www.abc.net.au/local/stories/2012/03/02/3444624.htm?site=sydney

62. *March 2, Associated Press* – (Wisconsin) **DNR blames bluff collapse on no pond liner.** Wisconsin state regulators investigating a bluff collapse at a Milwaukee-area power plant October 31, 2011 said a "significant factor" may have been the lack of a liner in a storm-water pond. The Associated Press reported March 2 the Wisconsin Department of Natural Resources (DNR) said We Energies may have violated regulations when it built a pond in and above a coal-ash landfill on its Oak Creek site. The DNR issued a notice of violation March 1. The notice said the utility could face fines of up to $5,000 per day. A utility spokesman said the utility is disputing the finding about the liner. He said it did not think a liner was necessary in this case. The collapse swept mud and ash into Lake Michigan.
Source: http://www.leadertelegram.com/news/daily_updates/article_e1e5e774-6476-11e1-a1fa-0019bb2963f4.html

63. *March 1, St. Joseph News-Press* – (Missouri) **Holt County awaits levee repairs.** Though an $888,000 contract was awarded to repair a nearly 1-mile breach in one of its levees, Holt County, Missouri officials said little work has occurred, while other counties see progress. "Atchison County had four breaches — two inlets and two outlets. I have 32 breaches in the Corps levees and an additional 12 to 15 in the non-Corps levees," a Holt County clerk said. At a Corps meeting March 1, officials said because of the wide scope of the projects, deadlines have shifted. According to the Corps of Engineers, the Union Township Levee District, which was awarded the federal money, is currently the only one in Holt County given a notice to proceed with repairs. Corps officials stated they expect the breach to be closed by spring, giving no exact date.
Source: http://www.newspressnow.com/localnews/30585504/detail.html

[Return to top]

Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/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