Daily Open Source Infrastructure Report
6 February 2012

Top Stories

- The FBI said it launched an investigation into how the hacking group Anonymous broke into and obtained information from a sensitive conference call between the bureau and Scotland Yard. – *Fox News; Associated Press* (See item **31**)

- Half of all Fortune 500 companies and major U.S. government agencies own computers infected with the "DNS Changer" malware that redirects users to fake Web sites and puts organizations at risk of information theft, a security company said. – *Computerworld* (See item **40**)

Fast Jump Menu

PRODUCTION INDUSTRIES	SERVICE INDUSTRIES
• Energy	• Banking and Finance
• Chemical	• Transportation
• Nuclear Reactors, Materials and Waste	• Postal and Shipping
• Critical Manufacturing	• Information Technology
• Defense Industrial Base	• Communications
• Dams	• Commercial Facilities
SUSTENANCE and HEALTH	**FEDERAL and STATE**
• Agriculture and Food	• Government Facilities
• Water	• Emergency Services
• Public Health and Healthcare	• National Monuments and Icons

---

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 2, Johnston Patch* – (Rhode Island) **DEM hits landfill companies with $55,000 fine.** The Rhode Island Department of Environmental Management (DEM) issued a notice of violation against two companies that operate at the Central Landfill, a

citation that also carries a $55,000 fine. The DEM director said in the statement the two firms, Rhode Island Resource Recovery Corporation and Broadrock Gas Services, "failed to maintain the landfill and the landfill gas collection and treatment systems" resulting in a rotten egg smell that affected Johnston and several neighboring communities. Broadrock also delayed telling the DEM that a "remote gas flare" used to burn off escaping landfill gas had stopped working, according to the statement. Instead of notifying the DEM within 1 hour as required by the company's pollution permit, Broadrock did not contact DEM about the failure until 5 days after the breakdown. Under other terms of the violation notice, the companies can no longer use construction debris — which contains sulfur, a main ingredient in the stench from the landfill — and must use a covering called Posi-Shell to seal the areas where the gases have been escaping.
Source: http://johnston.patch.com/articles/dem-hits-landfill-companies-with-55-000-fine

2. *February 2, WITI 6 Milwaukee* – (Wisconsin) **9,000 gallons of jet fuel collected from pipeline leak.** The 9,000 gallons of jet fuel that leaked out of a pipeline at Mitchell International Airport in Milwaukee, has been collected, WITI 6 Milwaukee reported February 2. The Wisconsin Department of Natural Resources (DNR) said the leak went unnoticed for roughly 2 weeks and could have spilled into the waterway nearby. Currently, officials see no immediate environmental concerns as a result of the leak — and officials said it is clear the leak never reached Lake Michigan. Officials determined the fuel was leaking from the airport grounds and flowing into Wilson Creek and the sewer system. However, as a precaution, there are skimmers on the creek near Howell and Layton Avenue to pick up any additional fuel in the water. To fix the problem and prevent further leakage, one of the airport runways was scheduled to be shut down February 3 while repairs are made.
Source: http://fox6now.com/2012/02/02/9000-gallons-of-jet-fuel-leaked-from-pipeline-at-airport/

3. *February 2, Nashville Tennessean* – (Tennessee) **Downed tree causes large fuel spill near Old Hickory Lake.** The storms that marched through Middle Tennessee February 1 caused crews to rush to clean up a large fuel spill caused by a downed tree near Old Hickory Lake in Wilson County, emergency officials said. The tree fell on four pipelines, said a battalion chief at Wilson Emergency Management Agency. "One carried diesel fuel, two carried gasoline, and one was electrical. All of these lines were about an inch and a half think and ran from the tank storage area at the yacht club down to the water, where the[y] fed the service tanks for boats." The tree damaged all four pipelines, but only caused two of them to leak. It was estimated that under 50 gallons leaked from the gasoline pipeline, and 400-600 gallons leaked from the diesel pipeline. Emergency officials were notified of the situation at about 10 a.m. February 2, when yacht club workers arrived to do their morning checks.
Source: http://www.tennessean.com/article/20120202/NEWS01/120202032/Downed-tree-causes-large-fuel-spill-near-Old-Hickory-Lake-

4. *February 2, Associated Press* – (Iowa) **Council Bluffs ethanol plant to pay $10,000 fine for Clean Air Act violation, buy equipment.** Owners of a Council Bluffs, Iowa

ethanol plant agreed to pay a fine for failing to implement risk management regulations required under the Clean Air Act, the Associated Press reported February 2. Southwest Iowa Renewable Energy LLC will pay a $10,000 penalty and spend at least $38,000 to purchase emergency response equipment for the Council Bluffs and the Lewis Township fire departments to settle the case with the Environmental Protection Agency (EPA). The EPA said a January 2010 inspection of the plant found no risk management plan on file. Such a plan is required because the plant stores more than 10,000 pounds of anhydrous ammonia, a hazardous chemical. The plant was storing about 28,000 pounds. The Clean Air Act rules are designed to prevent accidental chemical spills and minimize damage when there is a spill.
Source:
http://www.therepublic.com/view/story/c6a780d5a458471daa0d351b5b7d6dc3/IA--Ethanol-Plant-Fine/

[Return to top]

Chemical Industry Sector

5. *February 1, ICIS* – (International) **US alleges DuPont TiO2 technology stolen for China.** A man was ordered to stay in a U.S. jail February 1 in connection with an alleged scheme to steal titanium dioxide (TiO2) trade secrets from DuPont on behalf of Chinese government officials. A federal judge in San Francisco ordered the businessman to remain in detention as a flight risk pending trial, said a spokesman for the U.S. attorney's office. Prosecutors opposed his release and alleged in a court document that investigators found a "trove of evidence â□¦ which shows [he] was selling trade secrets belonging to [DuPont] to companies controlled by the government of the People's Republic of China." The man was charged with witness tampering, conspiracy to tamper with witnesses, and making a false statement in connection with the U.S. probe. Prosecutors said they have evidence showing he obtained over $20 million from the sale of TiO2 technologies to Chinese companies.
Source: http://www.icis.com/Articles/2012/02/01/9528663/us-alleges-dupont-tio2-technology-stolen-for-china.html

For another story, see item **4**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *February 3, Nuclear Street* – (California) **Extensive wear found in recently replaced SONGS steam generator.** Just 2 years after it was replaced, the Nuclear Regulatory Commission (NRC) has reported significant wear in a steam generator at San Diego County, California's San Onofre Nuclear Plant, Nuclear Street reported February 3. Earlier the week of January 30, San Onofre unit 3 was taken out of service because of a leaking steam generator tube that resulted in a small release of radioactive steam into an auxiliary building. Initial reports from NRC inspectors February 2 also outlined wear in similar equipment at neighboring unit 2. During a scheduled outage for

maintenance and inspections, the NRC found the thickness of two tubes in one of unit 2's two steam generators had been worn away by a third. Of 9,700 tubes in the steam generator, 69 were found to be at least 20 percent worn, and 800 tubes were at least 10 percent worn. An NRC spokesman told the Associated Press accelerated wear in the early years of a steam generator's life is not unprecedented, and inspectors will conduct further tests.
Source:
http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2012/02/03/extensive-wear-found-in-recently-replaced-songs-steam-generator-020301.aspx

[Return to top]

Critical Manufacturing Sector

7. *February 2, KTRK 13 Houston* – (Texas) **Two-alarm fire at tool company east of downtown.** Fire crews were dispatched February 2 to the scene of a two-alarm fire at the Texas Tool Company in Houston. Firefighters arrived to find smoke and flames pouring out of the building. A portion of the roof reportedly caved in. The Houston Fire Department said that although hazardous material units responded, there were no chemicals involved. Officials did not know what started the fire. A nearby building was also evacuated. One firefighter suffered minor injuries battling the blaze.
Source: http://abclocal.go.com/ktrk/story?section=news/local&id=8528873

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

8. *February 3, Reuters* – (International) **U.S. indicts Wegelin bank for helping Americans avoid tax.** The United States indicted Wegelin, the oldest Swiss private bank, on charges it enabled wealthy Americans to evade taxes on at least $1.2 billion hidden in offshore bank accounts, the U.S. Justice Department said February 2. The announcement, made by federal prosecutors in Manhattan, New York, represents the first time an overseas bank was indicted by the United States for enabling tax fraud by U.S. taxpayers. The indictment said the U.S. government seized more than $16 million from Wegelin's correspondent bank, the Swiss giant UBS AG, in Stamford, Connecticut, via a separate civil forfeiture complaint. Because Wegelin has no branches outside Switzerland, it used correspondent banking services, a standard industry practice, to handle money for U.S.-based clients. The charges against Wegelin are fraud and conspiracy. Wegelin "affirmatively decided to capture for Wegelin the illegal U.S. cross-border banking business lost by UBS and deliberately set out to open new

undeclared accounts for U.S. taxpayer-clients leaving UBS," the indictment said. The indictment also accused Wegelin of helping two unnamed Swiss banks "repatriate undeclared funds to their own U.S. taxpayer-clients by issuing checks drawn on Wegelin's Stamford correspondent account." The transfers were separated into chunks below the $10,000 threshold at which such transfers are reported to the Internal Revenue Service. Wegelin, the indictment said, "co-mingled" the repatriated funds with other, unrelated funds, to better conceal their origin and nature. The charges against Wegelin were filed as a superseding indictment of three previously charged Wegelin bankers, naming several unindicted co-conspirators.
Source: http://www.reuters.com/article/2012/02/03/us-usa-tax-swiss-indictment-idUSTRE81203M20120203

9. *February 2, Chicago Tribune* – (National) **Motorola Solutions settles securities fraud suit for $200M.** Motorola Solutions Inc. will pay $200 million to settle a 2007 securities fraud lawsuit brought by shareholders. Attorneys representing the shareholders disclosed the proposed settlement February 2, which was also filed with a federal court in Chicago where the case was brought. The settlement is subject to court approval. The suit alleged Motorola artificially inflated its stock by misrpresenting the company's projected revenue for the third and fourth quarter of 2006. Motorola Solutions inherited the litigation after it split in 2011 from the cellphone business now known as Motorola Mobility. In December, the mediator proposed that Motorola Solutions settle for $200 million, which the parties accepted, according to court papers. The plaintiffs were led by the Macomb County Employees' Retirement System, and St. Clair Shores Police and Fire Pension System. Shareholders who acquired stock between July 19, 2006, and January 4, 2007, may be eligible for a recovery.
Source: http://articles.chicagotribune.com/2012-02-02/business/chi-motorola-solutions-settles-securities-fraud-suit-for-200m-20120202_1_motorola-solutions-securities-fraud-robbins-geller-rudman

10. *February 2, Easton Express-Times* – (Pennsylvania) **Threats to shoot Wells Fargo manager prompt locked doors at Monroe County branch, police say.** Staff at a bank in Monroe County, Pennsylvania, locked the doors February 2 and let customers in one at a time after a man made repeated threats that he was going to come in and shoot the bank manager, Pennsylvania State Police said. Troopers located the suspect at his home and took him into custody without incident, according to a news release. He was sent to Monroe County Prison to await arraignment on a charge of making terroristic threats. State police said they were called to a Wells Fargo branch in Chestnuthill Township just before 4:30 p.m. for a report of a man making threatening comments to bank employees. The threats "caused the employees to become frightened and they locked the interior doors and were letting customers in one at a time," police said in the news release.
Source: http://www.lehighvalleylive.com/slate-belt/index.ssf/2012/02/threats_to_shoot_wells_fargo_m.html

For another story, see item **16**

Transportation Sector

11. *February 3, Mitchell Daily Republic* – (South Dakota) **Truck hits bridge on I-90; tank rolls into median.** A semi-truck driven collided with a bridge February 2 on Interstate 90 in South Dakota. The incident occurred around 9:20 a.m. near mile marker 191, about 1 mile west of Murdo. The truck was hauling an empty 30,000-gallon oil tank when it collided with a bridge running over the interstate. The tank broke loose from the truck upon impact with the bridge and rolled into the median. Officers with South Dakota Highway Patrol and the Jones County Sheriff's Office responded. Officials with the South Dakota Department of Transportation were called to assess the damage to the bridge. They decided the bridge would have to be closed until repairs could be made. An estimate of how long the repairs will take has not yet been determined. The driver was issued a citation for violating the permit he was given to drive the oversize load through South Dakota. The highway patrol reported a crane would be needed to remove the wrecked tank from the median and place it on another truck to be hauled away.
Source: http://www.mitchellrepublic.com/event/article/id/61865/group/homepage/

12. *February 3, CBS; Associated Press* – (Colorado; Nebraska) **Heavy snowstorm hits Colo. on its way east.** A powerful winter storm swept across Colorado February 3 as it headed east, bringing blizzard warnings to eastern Colorado and western Kansas, and winter storm warnings for southeast Wyoming and western Nebraska. The storm stretched as far south as New Mexico, where transportation officials reported difficult driving conditions on several state highways. The Colorado Avalanche Information Center issued a warning through February 3 east of the Continental Divide, saying 2 feet of snow or more could overwhelm a weak snow pack, with natural and human-triggered avalanches likely February 3. The storm forced the cancellation of more than 600 arriving and departing flights at Denver International Airport that had been scheduled through February 3. That is about 35 percent of its average daily operations of 1,700 flights. Southwest Airlines canceled all its flights through 4 p.m. because of the storm. The airline said it wanted to mitigate the impact of the storm on its operations elsewhere across the country. The Colorado Department of Transportation closed portions of Interstate 70 east of Denver International Airport to Limon, stranding truckers. Interstate 25 north and south reopened after numerous accidents were cleared. The University of Colorado closed its Boulder campus, affecting about 30,000 students. Colorado lawmakers cancelled legislative work February 3. Many school districts announced they would be closed February 3, including the two largest, in Jefferson County and Denver.
Source: http://www.cbsnews.com/8301-201_162-57371140/heavy-snowstorm-hits-colo-on-its-way-east

13. *February 2, Fierce Homeland Security* – (National) **FTA lacks rail safety data, says OIG.** The Federal Transit Administration (FTA) lacks the data necessary to nationally oversee transit safety, said the Transportation Department Office of Inspector General (OIG) in a January 31 report. The Transportation Secretary in 2009 called on Congress to approve legislation giving the FTA a direct role in setting rail transit safety standards and overseeing their implementation in localities that take federal rail dollars.

Currently, 28 oversight agencies oversee 35 light rail and 13 heavy rail systems operated by 48 transit agencies across the country, leading to a disparity in standards such as rail car crash-worthiness and train operator certification. The only way the FTA would be able to step into an expanded oversight role would be to adopt data-driven, risk-based oversight, the OIG report says. But, while the FTA captures basic safety incident data such as fatalities and injuries, it does not have detailed information on matters such as the condition of rail transit assets. Were the FTA to increase its responsibilities, it would also have to institute new practices to ensure data quality, a problem that has plagued other Transportation Department regulators such as the Federal Highway Administration, the report adds. The agency would also face the difficult task of articulating a uniform set of national safety performance measures, since without standardization in the measures, it would be unable to assess how well local agencies do. Even without expanded authority, the report recommends the FTA improve its data collection, an effort FTA officials say they are undertaking in an assessment of current data gaps.
Source: http://www.fiercehomelandsecurity.com/story/fta-lacks-rail-safety-data-says-oig/2012-02-02

14. *February 2, New York Daily News* – (Alaska; International) **Scientists worry Alaska volcano, 'Cleveland', could blow soon.** Scientists in Alaska are worried that a massive volcano on a remote island about 1,000 miles southwest of Anchorage is primed to erupt and spew a giant ash plume that could paralyze intercontinental travel. The Alaska Volcano Observatory January 31 bumped the alert status for the Cleveland Volcano from yellow to orange — one step below the highest alert level. "Renewed eruptive activity of Cleveland Volcano has been observed in satellite data," the observatory said, noting a new 130-foot lava dome — a visible bulge of gathering lava — had formed in the mountaintop's crater. About 90 percent of air freight from Asia to North America and Europe flies over Alaska, along with some 20,000 commercial travelers a day, according to CNN. Experts say a significant eruption could lead to a shutdown of the airspace, sparking the worst travel nightmare since a giant ash curtain from an Iceland volcano grounded millions of global travelers in April 2010.
Source: http://www.nydailynews.com/news/national/scientists-worry-alaska-volcano-cleveland-blow-article-1.1015974

15. *February 2, Reuters* – (Alaska) **Avalanche closes sole highway out of Anchorage.** The sole highway leading south from Anchorage, Alaska, was closed February 2 after an early-morning avalanche swept through the mountains and over the road, state officials said. Authorities said it was unknown how long the Seward Highway would remain closed, essentially cutting off travel between Anchorage and the Kenai Peninsula cities of Seward and Homer. Rapidly warming temperatures, high winds, and new snow and rain have created dangerous avalanche conditions throughout the region's Chugach Mountains, which are already loaded with near-record amounts of snow. "We consider the risk level at `considerable' at this point in time," said a spokesman for the state department of transportation and public facilities. That designation means small to moderate avalanches are likely, he said. The department has advised motorists to avoid travel along the route, the mountain-lined Seward Highway, if possible. Backcountry travelers were also warned by managers of the Chugach

National Forest that there are high to considerable risks of avalanches in the mountains south of Anchorage.
Source: http://www.chicagotribune.com/news/sns-rt-us-alaska-avalanchetre8112ec-20120202,0,7306651.story

For another story, see item **2**

Postal and Shipping Sector

16. *February 1, Contra Costa Times-Standard* – (Texas) **Alamo post office worker gets 18 months in prison in counterfeiting case.** A man who worked at the Alamo, Texas post office was sentenced January 31 to 18 months in prison for stealing $43,500 from the post office by using counterfeit bills to buy money orders, officials said. The man was convicted by a jury October 27, according to a news release from the U.S. attorney's office. He must also pay restitution of $39,973, the remaining balance owed to the Alamo Post Office, according to the release. He was convicted of stealing $13,800 from the post office by using counterfeit $100 bills to get money orders in February and March 2011. At sentencing, prosecutors presented evidence that he had stolen another $29,700 by using similar counterfeit bills at the post office starting in October 2010, according to court records. He also deposited similar counterfeit bills at the Provident Credit Union in Hayward and Oakland as early as August, 2010, according to court records.
Source: http://www.mercurynews.com/news/ci_19870713?source=rss

Agriculture and Food Sector

17. *February 3, Hutchinson News* – (Kansas) **Elevator explosion sends one to hospital.** Federal inspectors were on the scene in Arlington, Kansas, February 2 after a grain elevator explosion was reported at the Cairo Co-op, sending one worker to a hospital burn unit with serious injuries. Investigators from the Occupational Safety and Health Administration were at the elevator February 2. The Reno County Emergency Management director said an elevator employee opened an elevator door to go inside to conduct an inspection when the explosion occurred. He said it could be a few days before a cause could be determined. Emergency officials evacuated a 3-block area near the elevator. The evacuation was a precaution as firefighters put out a fire inside the elevator. Firefighters reported damage to the ground level of the structure, as well as embers and sparks coming from the elevator headhouse. The explosion blew out windows in the headhouse and a large metal overhead door at ground level.
Source: http://www.salina.com/news/story/Elevator-explosion-2-2-122012-02-03T01-03-30

18. *February 3, Food Safety News* – (National) **Hard-cooked egg recall widens.** Wegmans Food Markets, Greencore USA, and Allison's Gourmet Kitchens

have been caught up in the widespread recall of hard-cooked eggs that may be contaminated with Listeria, Food Safety News reported February 3. The expanded call back is the result of a recall by Minnesota-based Michael Foods, which produced the cooked eggs at its Wakefield, Nebraska facility. There have been no confirmed reports of illness. Wegmans is recalling certain hard-cooked eggs, as well as prepared foods that contain hard-cooked eggs. Greencore is recalling chefs salad. Allison's Gourmet Kitchens is recalling certain prepared potato, macaroni, pea, and egg salads. According to Michael Foods, the recall was initiated after lab testing revealed some eggs within three lot dates may have been contaminated with Listeria monocytogenes. A recall of those lot dates was announced January 26. The recall was expanded February 1 to include additional lot dates, which has prompted more recalls.
Source: http://www.foodsafetynews.com/2012/02/wegmans-recalls-hard-cooked-eggs-salads/

19. *February 3, Food Safety News* – (New York; New Jersey) **Allergen alert: Sulfites in tremella.** S&M USA Enterprise is recalling its Zhang Zhou-brand tremella because it may contain undeclared sulfites, Food Safety News reported February 3. Tremella is a kind of fungus used in Chinese cooking. Routine sampling by the New York State Department of Agriculture and Markets revealed the presence of sulfites in packages of the tremella, but sulfites were not listed on the label. People who have severe sensitivity to sulfites run the risk of serious or life-threatening allergic reactions if they consume them. The recalled Zhang Zhou brand tremella, which was imported from China, comes in an uncoded, 150-gram plastic bag and was sold in New York and New Jersey.
Source: http://www.foodsafetynews.com/2012/02/allergen-alert-sulfites-in-tremella/

20. *February 3, Food Safety News* – (National) **Uneviscerated imported fish recalled.** W & International Import Inc. is recalling certain sardine anchovies and dried yellow croaker imported from China because the fish were found to be uneviscerated, Food Safety News reported February 3. Fish that have not been fully gutted — uneviscerated — have been linked to outbreaks of botulism poisoning, because Clostridiuim Botulinum spores are more likely to be concentrated in the viscera than any other portion of the fish. The problem was discovered during routine sampling by the New York Department of Agriculture and Markets. The sale of uneviscerated fish is prohibited under department regulations. The recalled Rely-brand sardine anchovies were distributed nationwide.
Source: http://www.foodsafetynews.com/2012/02/uneviscerated-imported-fish-recalled/

21. *February 3, ABC News* – (National) **Is your orange juice safe?: FDA says carbendazim causes no safety concern.** After conducting new tests, the Food and Drug Administration (FDA) said low levels of a banned pesticide found in orange juice imported from Brazil is safe for sale in the domestic supply, according to a February 3 report from ABC News. The juice, which is stored in huge, 3-story high tanks in Florida, is tainted with the fungicide carbendazim, and will soon reach American grocery stores. The FDA has said that the juice is entirely safe to drink, and that the amount of the fungicide in the contaminated juice is far below unsafe levels. To test

positive for the pesticide, orange juice samples had to contain at least 10 parts per billion of the pesticide. Carbendazim has been found to cause birth defects in rodents and some chromosome problems in human cells in laboratories. However, it has not been found to have any health effects for humans. Carbendazim is a pesticide used to kill fungus and fungal spores. It is not approved for use on oranges in the United States, but is lawful in other countries. Studies show no risks of consuming carbendazim at up to 80 parts per billion, and that actual levels of danger are thousands of times higher, the Environmental Protection Agency said.
Source: http://abcnews.go.com/US/orange-juice-safe-fda-carbendazim-safety-concern/story?id=15504105#.TywDqMghxBl

22. *February 2, KOCO 5 Oklahoma City* – (Oklahoma) **Salmonella outbreak tied to fast-food chain.** There are new details about a salmonella outbreak now tied to Taco Bell, KOCO 5 Oklahoma City reported February 2. Oklahoma health officials released the information after the Centers for Disease Control (CDC) refused to release it. The CDC cited a longstanding policy against revealing the source of an outbreak after the threat is over. The outbreak at the end of 2011 made 68 people sick. There were 16 cases in Oklahoma and the state health department connected 8 of those to Taco Bell. Out of the 16 people who were infected with salmonella, four were hospitalized, according to state health officials. The outbreak was the third tied to Taco Bell in recent years. Taco Bell responded to the latest outbreak saying it thinks the salmonella came from one of its food suppliers. The CDC also said the threat of any more salmonella cases connected to this outbreak was over.
Source: http://www.koco.com/r/30357955/detail.html

23. *February 2, Food Safety News* – (National) **Maryland confirms Campylobacter in dairy's raw milk.** Maryland public health officials said lab tests confirmed Campylobacter jejuni bacteria in two unopened containers of unpasteurized milk from the Your Family Cow farm in Pennsylvania, Food Safety News reported February 2. Pennsylvania health authorities have not yet announced the results of their tests, as the number of people who are sick after drinking milk from the raw milk dairy has risen to 35. The confirmed cases of Campylobacter infection include 28 people in Pennsylvania, 4 in Maryland, 2 in West Virginia, and 1 in New Jersey. The owners of Your Family Cow farm, one of the largest raw milk dairies on the East Coast, said tests conducted on three samples of milk by a private lab they retained were negative for pathogens.
Source: http://www.foodsafetynews.com/2012/02/maryland-confirms-campylobacter-in-dairys-raw-milk/

For another story, see item **24**

Water Sector

24. *February 3, U.S. Geological Survey* – (National) **Irrigation causing declines in the High Plains Aquifer.** Groundwater withdrawals for crop irrigation have increased to

over 16 million acre-feet per year in the High Plains Aquifer, according to a recent U.S. Geological Survey (USGS) study released February 3. The USGS study shows recharge, or the amount of water entering the aquifer, is less than the amount of groundwater being withdrawn, causing groundwater losses in this already diminished natural resource. Crop irrigation is the largest use of groundwater in the aquifer, and, over the past 60 years, has caused severe water-level declines of up to 100 feet in some areas. The new USGS findings address concerns about the long-term sustainability of the aquifer. The High Plains aquifer underlies about 175,000 square miles in parts of eight states – Colorado, Kansas, Nebraska, New Mexico, Oklahoma, South Dakota, Texas, and Wyoming – and is a major source of groundwater irrigation in the region. The High Plains region supplies about one-fourth of the nation's agricultural production. The new USGS study also compares previously published data with new methods for estimating recharge and groundwater withdrawals, and provides an assessment of the strengths and weaknesses of those methods. This USGS report is part of a larger study to evaluate groundwater availability of the High Plains Aquifer.
Source: http://www.wateronline.com/article.mvc/Irrigation-Causing-Declines-In-The-High-0001

25. *February 2, Santa Rosa Press Democrat* – (California) **Sonoma County Water Agency officials declare Russian River supply 'dry'.** Dismal rainfall totals have prompted the Sonoma County Water Agency of California to formally change the designation for the Russian River water supply from "normal" to "dry," allowing officials to withhold water in Lake Mendocino and reduce Russian River water flows. The decision is intended to ensure storage of enough water to support consumer needs and permit releases into the river during the fall Chinook salmon migration, the water agency said. Storage in Lake Mendocino is at 89 percent of water supply capacity, and storage in Lake Sonoma is at 84 percent of capacity. Lake Pillsbury on the Eel River, however, is not quite at 45 percent of water supply capacity, an indicator of low cumulative rainfall that triggered the "dry" designation under a 1986 decision by the state water resource control board, the water agency said.
Source:
http://www.pressdemocrat.com/article/20120202/ARTICLES/120209923/1010/sports?Title=Water-officials-declare-Russian-River-supply-dry-&tc=ar

26. *February 2, WWMT 3 Kalamazoo* – (Michigan) **New spill on Kalamazoo River raises water safety questions.** The U.S. Environmental Protection Agency (EPA) estimates that several hundred gallons of diesel fuel, or something similar spilled into the Kalamazoo River in Michigan, and could threaten a community's drinking water. The spill was spotted February 1 in a drainage ditch in Battle Creek and now the EPA believes it has reached as far as Galesburg. The EPA said there was a nearly identical spill in the same place in February 2011, but they still do not know where it is coming from. Between the Enbridge oil spill and these two unexplained diesel spills, there have been a lot of toxic chemicals heading down the Kalamazoo River, which wraps itself right around Augusta's water wells and the village is not sure what to do. Officials said the effects are running right by Augusta's water wells, and that could be a problem for the more than 1,000 people who depend on them. For now, the village plans to continue working with the EPA and the state department of natural resources to monitor its

water supply.
Source: http://www.wwmt.com/articles/suspected-1401294-kalamazoo-battle.html

For another story, see item **2**

Public Health and Healthcare Sector

27. *February 3, Infosecurity* – (National) **Number of patient record data breaches nearly doubled last year.** The total number of patient records compromised in the United States increased by 97 percent in 2011 compared with 2010, according to a report released this week by the Redspin consulting firm. Redspin cites the increasing concentration of protected health information (PHI) on unencrypted portable devices and the lack of sufficient oversight of PHI disclosed to hospital's business associates as the main reasons for the increase. Malicious attacks (theft, hacking, and insider incidents) continue to cause 60 percent of all breaches due to the economic value of personal health records sold on the black market, and for medical ID theft used to commit Medicare fraud. Redspin examined data breach information on the U.S. Department of Health and Human Services Web site, which lists a total of 385 breaches affecting more than 19 million individuals since breach reporting notification requirements went into effect in August 2009. For a breach to be reported, it must affect 500 individuals or more. In addition, the average number of records affected by a single breach has almost doubled.
Source: http://www.infosecurity-us.com/view/23648/number-of-patient-record-data-breaches-nearly-doubled-last-year/

Government Facilities Sector

28. *February 2, Associated Press* – (South Carolina) **SC college student charged with fire bombings.** A senior at the University of South Carolina (USC) was arrested and accused of throwing seven explosive devices at buildings on campus and in downtown Columbia, South Carolina. The 22-year-old senior from Columbia was arrested February 1. Police said he made homemade bombs and threw them from parking garages at vacant houses and trash bins. Police believed one of the devices was thrown at a bar in Columbia that caused $300,000 in damage. USC police filed three charges of possessing and using an incendiary device. Four of the charges came from the Columbia Fire Department. Police said they found bottles, rags, and gas cans after a search of the suspect's apartment.
Source: http://www.citizen-times.com/article/20120202/NEWS/302020041/SC-college-student-charged-fire-bombings?odyssey=mod|newswell|text|Frontpage|s

29. *February 2, WSPA 7 Spartanburg* – (South Carolina) **Foreign hackers attacking SC DMV database daily.** Foreign-based hackers were suspected in attacks on the South Carolina Department of Motor Vehicles' (DMV) computers, trying to obtain personal

information on millions of South Carolina drivers, WSPA 7 Spartanburg reported February 2. "We've had about 90 intrusion attempts since the beginning of this year," said the director of operations at the DMV. "We have deflected all of those attempts." The DMV contacted the FBI, since most of the hackers are attacking from foreign countries. The FBI's local cyber-security squad is assisting the DMV to make sure everything possible is being done to protect the DMV database, which contains not only drivers' names and addresses but also Social Security numbers and copies of birth certificates.
Source: http://www2.wspa.com/news/2012/feb/02/foreign-hackers-attacking-sc-dmv-database-daily-ar-3161441/

30. *February 1, San Franciso Examiner* – (California) **San Francisco tracing viral outbreak.** The highly contagious disease that has sickened 325 students and 30 staff members at St. Ignatius College Preparatory Academy might have been brought onto campus by a person, San Francisco city health officials said February 1. The deputy health officer said the agency believes the disease is viral, not foodborne, meaning someone was sick when they attended school. The school was closed February 1 for a deep cleaning after a high number of students called in sick with viral gastroenteritis, more commonly known as stomach flu. The school will remain closed until February 6 as a precaution, the school's principal said. Students were advised to not return to school until 3 days after their symptoms subside. The deputy health officer said the public health department is running tests to see if the school is dealing with a norovirus — which causes similar symptoms.
Source: http://www.sfexaminer.com/local/2012/02/san-francisco-tracing-viral-outbreak

For more stories, see items **12** and **40**

[Return to top]

Emergency Services Sector

31. *February 3, Fox News; Associated Press* – (International) **Hackers claim to have intercepted call between FBI, Scotland Yard.** A sensitive conference call between the FBI and Scotland Yard was recorded by the hacking group Anonymous, it claimed February 3. The group released a roughly 15-minute-long recording of what appears to be a January 17 conference call devoted to tracking and prosecuting members of the loose-knit hacking group. There was no classified information on the call, FBI sources told Fox News, noting unsecure phones are not used for sensitive information. The source indicated those responsible will be held accountable. Names of some of the suspects being discussed were apparently edited from the recording. "The information was illegally obtained and a criminal investigation is underway," a FBI spokesman told Fox News. Anonymous also published an e-mail purportedly sent by an FBI agent that gave details and a password for accessing the call. Amid the material published by the hackers was a message purportedly sent by an FBI agent to international law enforcement agencies. It invites his foreign counterparts to join the call to "discuss the on-going investigations related to Anonymous ... and other associated splinter groups." The e-mail contained a phone number and password for accessing the call. The e-mail

was addressed to officials in England, Ireland, the Netherlands, Sweden, and France, but only American and British officials can be heard on the recording.
Source: http://www.foxnews.com/scitech/2012/02/03/hackers-claim-to-have-intercepted-call-between-fbi-scotland-yard/?test=latestnews

32. *February 3, Westmoreland Times* – (Pennsylvania) **Westmoreland County man charged with threatening FBI agent.** A resident of Youngwood, Pennsylvania, was indicted by a federal grand jury in Pittsburgh on a charge of violating a federal law involving threats against a federal agent, a U.S. attorney announced February 3. The one-count indictment, returned January 31, named the 44-year-old as the sole defendant. According to the indictment, on or about January 5, the man threatened to assault and murder a special agent of the FBI due to the performance of the agent's official duties. The law provides for a maximum sentence of 10 years in prison, a fine of $250,000, or both.
Source: http://westmorelandtimes.com/news/2012/02/westmoreland-county-man-charged-with-threatening-fbi-agent-03021208191801/

33. *February 2, Syracuse Post-Standard; Associated Press* – (New York; Utah; Texas) **'Anonymous' hackers shut down Syracuse police Website.** Hackers affiliated with the group "Anonymous" hacked the police Web site in Syracuse, New York and in Salt Lake City, and Texas, according to Syracuse police. The Syracuse public information site was hacked, but that did not include police reports or other sensitive information, said a sergeant. The Web site, www.syracusepolice.org, will likely be shut down for a few days, he said. Syracuse police department names and apparent passwords were posted February 1 to sites where hackers often post snippets of code. The hackers cited the department's knowledge of a case, as well as the case of a former Auburn police officer, a convicted felon suing the city of Auburn for back pay and pension. The officer's case is not related to the Syracuse Police Department in any way. The sergeant stressed the hacked site was maintained by a third-party host and was not linked to departmental records. In Salt Lake City, hackers who broke into the police department site compromised more data than originally thought, police said February 1. "We have learned that citizen complaints regarding drug crimes in the community were also accessed. These forms included phone numbers, addresses, e-mail addresses, other personal information, and details about suspicious activity from a variety of sources," a news release stated. The hackers also attacked Texas police agencies, especially in the Fort Worth area.
Source: http://www.syracuse.com/news/index.ssf/2012/02/anonymous_hackers_shut_down_sy.html

34. *February 1, Chicago Journal* – (Illinois) **Rowdy arrestee pulls fire alarm.** A woman added to her troubles after trying to escape from a police station the morning of January 29. While being transported from a lock-up area at the 1st District police station in Chicago after being arrested for a bail bond violation for other charges, she reportedly struck a detention aide in the head and pulled a fire alarm in the facility in an attempt to escape. She was apprehended before she could get out of the building, and officers brought her back to the lock-up area. According to the report, she damaged the fire

alarm unit.
Source: http://www.chicagojournal.com/News/02-01-2012/Rowdy_arrestee_pulls_fire_alarm

For another story, see item **4**

Information Technology Sector

35. *February 3, IDG News Service* – (International) **Symantec warns of Android trojans that mutate with every download.** Researchers from Symantec identified a new premium-rate SMS Android trojan that modifies its code every time it gets downloaded to bypass antivirus detection. This technique is known as server-side polymorphism and already existed in the world of desktop malware for many years, but mobile malware creators have only now begun to adopt it. A special mechanism that runs on the distribution server modifies certain parts of the trojan to ensure every malicious app that gets downloaded is unique. This is different from local polymorphism where the malware modifies its own code every time it gets executed. Symantec identified multiple variants of this trojan horse, which it detects as Android.Opfake, and all of them are distributed from Russian Web sites. However, the malware contains instructions to automatically send SMS messages to premium-rate numbers from many European and former Soviet Union countries. In some cases, especially when security products rely heavily on static signatures, detecting malware threats that make use of server-side polymorphism can be difficult.
Source:
http://www.computerworld.com/s/article/9223950/Symantec_warns_of_Android_Trojans_that_mutate_with_every_download?taxonomyId=17

36. *February 3, The Register* – (International) **Satellite phones lift skirt, flash cipher secrets at boffins.** Two researchers at the Ruhr-University Bochum managed to extract secret encryption algorithmns used by satellite phones, and discovered they are a lot less secure than one might think.They analyzed firmware updates for popular satellite handsets to extract ciphers used by the Thuraya and Inmarsat networks, which are known as GRM-1 and GRM-2 respectively. The first cipher turned out to be a variant of the already-exploited A5/2 cipher on which GSM used to depend; GRM-2 has not been attacked yet, but the researchers believe it would not be difficult to break. Modern security systems, including SSL and modern GSM networks, use published ciphers that are open to general scrutiny, but there was a point when it was considered better to keep the method by which data is encrypted secret as an additional barrier. Now, however, attackers can identify secret ciphers, and the lack of public analysis made for much weaker ciphers that were subsequently broken. GSM, for example, used secret ciphers that turned out to have exploitable weaknesses, so now (in most places) shifted to the A5/3 cipher, which is widely published, tested, and proved resistant to assault. However, satellite systems have not moved on as quickly, and the researchers' job was made easier by the short production run of satellite handsets. GSM cryptography is almost all done in hardware, the quantity of GSM phones makes it economical to

fabricate specialist silicon for the job, but satellite phones do the same work in software so the ciphers can be found within firmware updates.
Source: http://www.theregister.co.uk/2012/02/03/satellite_phone_hack/

37. *February 3, IDG News Service* – (International) **PHP 5.3.10 fixes critical remote code execution vulnerability.** The PHP Group released PHP 5.3.10 February 2 to address a critical security flaw that can be exploited to execute arbitrary code on servers running an older version of the Web development platform. The vulnerability is identified as CVE-2012-0830 and was discovered by an independent security consultant and creator of the popular Suhosin security extension for PHP. SecurityFocus classifies the issue as a design error because it was accidentally introduced while fixing a separate denial-of-service (DoS) vulnerability in early January. That vulnerability is known as CVE-2011-4885 and was disclosed in December. It affects a number of Web development platforms, including PHP, ASP.NET, Java, and Python and can be exploited in a so-called hash collision attack. The PHP development team addressed CVE-2011-4885 in PHP 5.3.9, released January 10. The error can be exploited by attackers to remotely execute arbitrary code on a system that runs a vulnerable PHP installation. PHP 5.3.9, along with any older versions for which the hash collision DoS patch was backported are affected, a chief security specialist at Secunia said. Proof-of-concept code that exploits the vulnerability was published online, so the likelihood of attacks targeting CVE-2012-0830 are high.
Source:
http://www.computerworld.com/s/article/9223955/PHP_5.3.10_fixes_critical_remote_code_execution_vulnerability

38. *February 2, U.S. Consumer Product Safety Commission* – (International) **HP recalls fax machines due to fire and burn hazards.** The U.S. Consumer Product Safety Commission, in cooperation with Hewlett-Packard (HP) announced a voluntary recall February 2 of about 928,000 HP fax 1040 and 1050 machines. The importer was Hewlett-Packard Co., of Palo Alto, California. The machines were manufactured in China. The fax machines can overheat due to an internal electrical component failure, posing fire and burn hazards. HP is aware of seven reports of machines overheating and catching fire, resulting in property damage, including one instance of significant property damage and one instance of a minor burn injury to a consumer's finger. Six incidents were reported in the United States. The machines were sold at electronics, computer, and camera stores nationwide, and online at www.shopping.hp.com and other Web sites from November 2004 through December 2011. Some of the recalled fax machines were replacement units for a previous recall involving HP fax model 1010 in June 2008.
Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12101.html

39. *February 2, Wired* – (International) **Google beefs up Android Market security.** Google unveiled a new security service for the Android Market February 2 that aims to auto-scan uploaded Android applications to detect potentially malicious apps more quickly, ideally before users download them. Codenamed Bouncer, the new service searches for threats without requiring any pre-approval process, continuing to keep the Market as "open" as it has always been. The new security service has already

been working for the past few months. After finding an app that violates the rules — be it malware or spyware — the Android team takes the application down and bans the developer account from uploading any more apps. Further, Google continues to check new Android developer account sign-ups, so repeat offenders will not continue to upload malicious apps under different user names.
Source: http://www.wired.com/gadgetlab/2012/02/google-android-malware-scanner/

40. *February 2, Computerworld* – (International) **Half of Fortune 500 firms infected with DNS Changer.** Half of all Fortune 500 companies and major U.S. government agencies own computers infected with the "DNS Changer" malware that redirects users to fake Web sites and puts organizations at risk of information theft, security company Internet Identity (IID) said February 2. DNS Changer, which at its peak was installed on more than 4 million Windows PCs and Macs worldwide — a quarter of them in the United States alone — was the target of a major takedown organized by the U.S. Department of Justice in November 2011. The takedown and accompanying arrests of six Estonian men, was dubbed "Operation Ghost Click." As part of the operation, the FBI seized control of more than 100 command-and-control servers hosted at U.S. data centers. According to IID, half of the firms in the Fortune 500, and a similar percentage of major U.S. government agencies, harbor one or more computers infected with DNS Changer. IID used telemetry from its monitoring of client networks, as well as third-party data, to claim at least 250 of the Fortune 500 companies and 27 out of 55 major government agencies had at least one computer or router infected with DNS Changer as of early 2012.
Source:
http://www.computerworld.com/s/article/9223941/Half_of_Fortune_500_firms_infected_with_DNS_Changer?taxonomyId=17

41. *February 2, Infosecurity* – (International) **Oracle patches denial-of-service vulnerability.** Oracle pushed out a patch for a denial-of-service vulnerability in the Oracle WebLogic Server, Application Server, and iPlanet Web Server due to hash collisions. Oracle warned in a security advisory the vulnerability might be "remotely exploitable without authentication," which means it might be exploited over a network without the need for username or password. Hash collisions occur when two distinct pieces of data have the same hash value. The company noted that a fix for the same vulnerability in the GlassFish Server was released in its quarterly patch update in January. In that update, Oracle shipped 78 patches across the full range of its products, including 2 fixes to its Database Server.
Source: http://www.infosecurity-magazine.com/view/23645/

For more stories, see items **9**, **29**, **31**, and **33**

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

Communications Sector

42. *February 2, United Press International* – (New York) **12 charged in cell phone cloning scam.** New York City prosecutors charged 12 people in a $250 million cellphone account cloning scam, United Press International reported February 2. A Manhattan U.S. attorney said "tens of thousands" of customer accounts were stolen and used in the black market international calling scam, according to the New York Daily News. The suspects allegedly used customer phone numbers and code numbers associated with the accounts to make cloned cellphones appear to be legitimate to service providers, the U.S. attorney said. Hardware from a Chinese company allowed the suspects to route international calls made with the illegal phones through the Internet at cheap rates, he said. He said five of the suspects were arrested February 1, while the rest remain at large. The investigation came out of a similar investigation by U.S. Secret Service agents that led to the arrest of nine Sprint employees who stole and sold customer information to clone scammers in 2010.
Source: http://www.upi.com/Top_News/US/2012/02/02/12-charged-in-cell-phone-cloning-scam/UPI-53861328214576/

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

Commercial Facilities Sector

43. *February 3, WJBK 2 Detroit* – (Michigan) **Arson suspected in commercial building fire on Detroit's east side.** One person was in police custody as fire crews in Detroit fought a fire at a large commercial building on the city's east side February 3. Video from the scene showed flames leaping from the building, which is located in an industrial area with homes nearby. A police sergeant said officers approached a man near the building carrying a large black trash bag that contained gas containers and clothing items which smelled of gasoline. He was arrested. Police said another suspect escaped on foot. Arson investigators were at the scene. Hazardous materials crews and emergency medical services also responded.
Source: http://www.myfoxdetroit.com/dpp/news/local/arson-suspected-in-commercial-building-fire-on-detroit's-east-side-20120203

44. *February 3, Associated Press* – (Maryland) **Four charged in fatal shooting at Towson mall.** Baltimore County police said four men caught on surveillance video trailing a teen through Towson Town Center mall in Towson, Maryland, just days before December 25 were charged in the fatal shooting of the teen just steps from the mall. Police announced the arrests in the slaying February 2. Surveillance video shows one of the suspects encountering the teen in a store and calling the second suspect. He then drove two other suspects to the mall, where police said the men communicated by phone while following the teen through the mall. Police said one of the suspects shot

the teen multiple times on the sidewalk outside Nordstrom as he left the mall. All four men are charged with first-degree murder.
Source: http://www.stardem.com/article_a262d806-2630-5fac-a8ab-3dd3b7b644b7.html

45. *February 3, Associated Press* – (South Carolina) **Area evacuated as SC police probe meth materials.** A shopping center and nearby roads in Surfside Beach, South Carolina, were evacuated for several hours after authorities checked out a car carrying chemicals used for making methamphetamines February 2. Police were called about a report of shoplifting at one of the stores in the shopping center. They later found the chemicals in the car and cleared the shopping center and nearby roads for about 2 hours. Two men and two women were arrested.
Source: http://www.foxcarolina.com/story/16669327/area-evacuated-as-sc-police-probe-meth-materials

46. *February 2, Visalia Times-Delta* – (California) **Morning fire in Visalia causes $40,000 in damage.** A fire that broke out February 2 destroyed a portion of a business in Visalia, California, causing thousands of dollars worth of damage. Visalia firefighters battled flames caused when a large metal trash bin caught fire. The flames spread to an awning that stretched over a parking lot that served a massage parlor, hair salon, and Clear Internet and Computer Repair. Fire officials believe the fire may have been intentionally set. They said a serial arsonist set metal trash bins on fire in 2011 in the same area. The man who owns the building that houses the three businesses said he estimated the damage at $40,000.
Source: http://www.visaliatimesdelta.com/article/20120203/NEWS01/202030311

For more stories, see items **3**, **28**, and **40**

National Monuments and Icons Sector

See item **15**

Dams Sector

47. *February 2, KAAL 6 Austin* – (Minnesota) **Lanesboro dam needs reconstruction.** The Lanesboro Power Dam on the Root River in Lanesboro, Minnesota, is in need of reconstruction, as it is putting the city at risk. The trouble began with a letter from the state department of natural resources stating the dam had to be fixed or torn down because it is high hazard, said a Lanesboro city administrator. The dam is at the center of a debate between the Lanesboro and the state's historic preservation office, which says because it is in a historic location it needs to be built with similar materials from when it was first built, making it a much more costly project for the city.
Source: http://kaaltv.com/article/stories/S2480678.shtml?cat=10219

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

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.