# Daily Open Source Infrastructure Report
# 9 April 2012

## Top Stories

- The Federal Aviation Administration is investigating an air traffic controller accused of ignoring a request for an emergency landing in Denver. The pilot reported smoke in the cabin of a United Express plane April 3. – *Associated Press* (See item **18**)
- The University of Pittsburgh evacuated four buildings April 5 after receiving a bomb threat. Over the last 3 weeks there have been 23 threats to university buildings, but no explosives have been found. – *WESA 90.5 FM Pittsburgh* (See item **32**)
- U.S. water and energy utilities face constant cyber-espionage and denial-of-service attacks, according to a DHS cyber response team, which took 17 fly-away trips in 2011 to assist utilities in network and forensics analysis. – *Network World* (See item **39**)
- A Navy fighter jet crashed into an apartment complex near Virginia Beach, Virgina, April 6. Both crew members and five civilians were taken to local hospitals. At least five buildings were heavily damaged. – *Raycom News Network* (See item **47**)
- New documents released the week of April 2 show that a cascade of missteps combined with weather conditions to produce the 6-square-mile fire that killed 3 people and destroyed dozens of homes near Denver. – *Associated Press* (See item **51**)

## Fast Jump Menu

**PRODUCTION INDUSTRIES**
- Energy
- Chemical
- Nuclear Reactors, Materials and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

**SUSTENANCE and HEALTH**
- Agriculture and Food
- Water
- Public Health and Healthcare

**SERVICE INDUSTRIES**
- Banking and Finance
- Transportation
- Postal and Shipping
- Information Technology
- Communications
- Commercial Facilities

**FEDERAL and STATE**
- Government Facilities
- Emergency Services
- 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. *April 5, Associated Press* – (Colorado) **Xcel blames road chemicals for Colorado power outages.** Xcel Energy is blaming chemicals used to keep roads clear of snow for outages that left up to 23,000 people in Colorado without power and heat, the Associated Press reported April 5. The company said emergency crews had to put out utility pole fires and clear downed power lines across the Denver metro area due to strong winds during an April 3 snowstorm. The company told KUSA 9 Denver dirt and magnesium chloride kicked by cars on the road piles up on power lines and can cause electricity to jump to the wood pole, catching it on fire.
Source: http://www.insurancejournal.com/news/west/2012/04/05/242363.htm

For another story, see item **39**

[Return to top]

## Chemical Industry Sector

2. *April 5, Twin Falls Times-News* – (Idaho) **No injuries reported in Idaho sulfur explosion.** No one was injured April 4 when sulfur buildup caused an auger atop a warehouse to explode at a Paul, Idaho fertilizer plant. A Minidoka County Sheriff's captain said there were workers near the auger when it exploded. According to emergency radio communication, smoke poured out the rear door of the company's warehouse after the explosion.
Source: http://www.firehouse.com/news/10689319/no-injuries-reported-in-idaho-sulfur-explosion

[Return to top]

## Nuclear Reactors, Materials and Waste Sector

3. *April 5, WCNC 36 Charlotte* – (South Carolina) **Power restored at Catawba nuclear plant.** The Catawba nuclear power plant near York, South Carolina, restored power April 5 after an overnight outage, according to the U.S. Nuclear Regulatory Commission (NRC) and Duke Energy. Duke said steam was vented following the shutdown of the Unit One reactor. There was no radiation released or impact to plant workers or the public after power was lost, but NRC staff were still monitoring the situation at the plant.
   Source: http://www.wcnc.com/home/Catawba-nuclear-power-plant-loses-power-146215425.html

For another story, see item **39**

[Return to top]

## Critical Manufacturing Sector

4. *April 5, KTVZ 21 Bend* – (Oregon) **Fire prompts Redmond metals plant evacuation.** Officials in Redmond, Oregon said a small fire April 5 at PCC Schlosser Castings could have been a lot worse, but employees took the right steps and evacuated the premises. A total of 25 to 30 employees were evacuated at the metals company that makes plane parts. Fire officials said titanium dust, which gets sucked up into a containment system and is very combustible, somehow caught fire. Fire officials said the fire was the third time something similar had happened at the facility.
   Source: http://www.ktvz.com/news/30845554/detail.html

5. *April 5, U.S. Department of Labor* – (Ohio) **U.S. Labor Department's OSHA proposes $151,300 in fines to Ohio-based American Showa for lack of personal protective gear, electrical hazards training.** The U.S. Department of Labor's Occupational Safety and Health Administration has cited American Showa Inc. with 13 safety and health violations at its Blanchester, Ohio facility, according to an April 5 news release. The facility manufactures power steering pumps and power steering gear boxes for the transportation industry. The willful safety violations included failing to train workers on safe electrical working practices for voltage testing and the use of required personal protective equipment. Seven serious safety violations and one other-than-serious violation were also cited.
   Source:
   http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22113

6. *April 5, U.S. Department of Labor* – (Pennsylvania) **U.S. Department of Labor's OSHA proposes more than $45,000 in fines to Wheatland, Pa., company for exposing workers to safety hazards.** The U.S. Department of Labor's Occupational

Safety and Health Administration (OHSA) has cited ACCI Acquisition Co. LLC, doing business as cylinder caps and related compressed gas cylinder products manufacturer American Cap Co. LLC, for 18 serious and 4 other-than-serious safety and health violations at the company's Wheatland, Pennsylvania facility, according to an April 5 news release. The violations followed an inspection conducted under the OSHA's Site-Specific Targeting Program for industries with high injury and illness rates. The serious violations included failing to ensure that spray guns are connected to the powder coating spray booth's ventilation system, provide effective welding equipment, ensure that compressed air is reduced to 30 pounds per square inch, equip the spray booth with an automatic sprinkler, protect workers from direct exposure to laser radiation, and provide proper eye protection for employees working around laser radiation.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22122

[Return to top]

## Defense Industrial Base Sector

7. *April 5, Framingham MetroWest Daily News* – (Massachusetts) **Ashland Police say white powder wasn't dangerous.** Ashland, Massachusetts police and the FBI are investigating the origins of an envelope filled with white powder that closed Nordost Corp. in Holliston and the Ashland Police Station April 4. The buildings were locked down and quarantined. No one was allowed in or out for about 2 hours until a state hazardous materials team said it was safe. An Ashland police official said the owner of Nordost Corp., which makes audio and video cables, came to the station with an envelope he said was suspicious. The envelope was addressed to an address in Washington, D.C., but it was returned to the sender, which was Nordost Corp. "He did not recognize the envelope or the address it was sent to," the police official said, adding that the owner recently relocated his business from Ashland to Holliston. The HAZMAT team tested the material, which did not test positive for any known dangerous material, the police official said. While the building was locked down, Ashland Police forwarded all of its calls to Hopkinton Police until the building was reopened.
Source:
http://www.metrowestdailynews.com/news/police_and_fire/x760620859/White-powder-clears-out-Ashland-Police-Department

[Return to top]

## Banking and Finance Sector

8. *April 6, U.S. Securities and Exchange Commission* – (Florida) **SEC charges south Florida man in investment fraud scheme.** The U.S. Securities and Exchange Commission (SEC) charged April 6 that a south Florida investment manager defrauded investors by making false claims about his investment track record and providing bogus

account statements that reflected fictitious profits. In the complaint, the SEC alleges that since 2005, the manager and International Consultants & Investment Group Ltd. Corp. pulled in at least $11 million from investors by falsely claiming annual returns as high as 26 percent, and that he transferred more than $2.5 million of investor funds to two entities he controlled, Elia Realty, Inc., and 212 Entertainment Club, Inc. He told investors that he had extensive experience in day trading stocks and exchange-traded funds, but his trading resulted in losses or only marginal gains, and the quarterly account statements he sent to clients overstated their returns, the SEC alleged. In a parallel criminal case, a U.S. attorney announced the manager was also indicted on one count of wire fraud.
Source: http://www.sec.gov/news/press/2012/2012-56.htm

9. *April 6, U.S. Securities and Exchange Commission* – (National; International) **SEC freezes accounts of six Chinese citizens and one offshore entity charged with insider trading.** The U.S. Securities and Exchange Commission (SEC) announced April 6 it has obtained a court-ordered freeze of the assets of six Chinese citizens and one British Virgin Islands entity charged with insider trading in Zhongpin Inc., a China-based pork processor whose shares trade in the U.S. The SEC's complaint, filed April 4 in a U.S. district court in Chicago, alleges the defendants reaped more than $9 million by trading in Zhongpin ahead of a March 27 announcement of a proposal to take the company private. The complaint names as defendants one entity, Prestige Trade Investments Ltd., and six individuals. The SEC alleged that one of the individuals formed Prestige in January and funded its U.S. brokerage account in March with $29 million transferred from a Hong Kong bank. According to the complaint, the seven defendants bought substantial quantities of common stock and call options in Zhongpin between March 14 and March 26. Zhongpin's stock price jumped 21.8 percent March 27 when the company publicly announced that its chairman and chief executive officer had made a non-binding offer to acquire all of Zhongpin's outstanding stock at $13.50 a share, a 46 percent premium over the previous day's closing price. "The defendants in this action – all with seemingly limited resources - suddenly and inexplicably purchased more than $20 million in Zhongpin securities just before an important public announcement," the director of the SEC's Chicago Regional Office said. The SEC alleges that the purchases of Zhongpin stock and options were inconsistent with the defendants' financial situations and prior investment behavior.
Source: http://www.sec.gov/news/press/2012/2012-54.htm

10. *April 6, Newark Patch* – (New Jersey; Georgia; South Carolina) **Man pleads guilty in mortgage fraud.** A man admitted April 5 in a Camden, New Jersey federal court to taking part in a $40.8 million mortgage fraud scheme in which he helped find phony buyers for vacation properties in New Jersey and two other states. He pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit money laundering. Authorities said the defendant recruited "straw buyers" for his co-conspirators to purchase oceanfront condominiums overbuilt by financially distressed developers in Wildwood Crest, as well as in vacation destinations in Georgia and South Carolina and properties in New Jersey owned by financially distressed homeowners facing foreclosure. His co-conspirators caused fraudulent mortgage loan applications and

supporting documents to be submitted to mortgage lenders in the straw buyers' names, attributing inflated income and assets to the buyers in order to induce the lenders to approve the loans. Once the loans were approved and the mortgage lenders sent the loan proceeds in connection with the real estate closings on the properties, the man and his co-conspirators took a portion of the proceeds from the fraudulent mortgage loans.
Source: http://newarknj.patch.com/articles/man-pleads-guilty-in-mortgage-fraud

11. *April 6, Associated Press* – (North Carolina) **FDIC sues failed Cape Fear Bank for $11 million.** Federal regulators sued several former directors and officers of North Carolina's failed Cape Fear Bank to recover more than $11 million in losses the bank suffered on 23 commercial loans. The Star-News of Wilmington reported that the suit filed April 4 by the Federal Deposit Insurance Corp. (FDIC) said the risky acquisition, development, and construction loans were approved between 2006 and 2009. The Wilmington-based bank failed in April 2009 and was taken over by First Federal of Charleston. The suit said the loans and other negligence caused the bank's losses. The FDIC wants to recover about $11.2 million plus interest and costs from the bank's former officers.
Source: http://www2.wnct.com/news/2012/apr/06/fdic-sues-failed-cape-fear-bank-for-11-million-ar-2134195/

12. *April 6, U.S. Securities and Exchange Commission* – (Texas) **SEC charges Texas bank holding company's CEO and CFO with misleading investors about loan quality and financial health during the financial crisis.** The U.S. Securities and Exchange Commission (SEC) announced April 6 it charged Texas-based Franklin Bank Corp.'s former chief executives for their involvement in a fraudulent scheme designed to conceal the deterioration of the bank's loan portfolio and inflate its reported earnings during the financial crisis. The SEC alleges that Franklin's former chief executive officer (CEO) and chief financial officer (CFO) used aggressive loan modification programs during the third and fourth quarters of 2007 to hide the true amount of Franklin's non-performing loans and artificially boost its net income and earnings. The Houston-based bank holding company declared bankruptcy in 2008. According to the complaint filed in a Texas district court April 5, as Franklin's holdings of delinquent and non-performing loans rose significantly in the summer of 2007, the CEO and CFO instituted three loan modification schemes that caused Franklin to classify those loans as performing. By the end of September 2007, they had used the loan modification programs to conceal more than $11 million in non-performing single family residential loans and $13.5 million in non-performing residential construction loans. As a result of the loan modifications, Franklin overstated its third-quarter 2007 net income and earnings by 317 percent, and 77 percent, respectively.
Source: http://www.sec.gov/news/press/2012/2012-55.htm

13. *April 5, Kansas City Star* – (Kansas; Missouri; National) **Raymore man admits to Petro America securities fraud, pleads guilty.** A man pleaded guilty April 5 in a U.S. district court in Kansas City, Kansas to participating in a $7.2 million securities fraud involving thousands of investors around the country who bought shares in Petro America Corp. He is the fourth defendant to plead guilty in the government's case

against Petro, which claimed to have assets in oil and 30 to 40 gold mines. According to a statement from the U.S. attorney's office, the man admitted he participated in a conspiracy to commit securities and wire fraud beginning in September 2008. He promoted Petro America and sold shares to investors, despite cease-and-desist orders from state securities regulators in Kansas and Missouri. He also was not licensed to sell securities. He made at least $172,774 from the sale of Petro stock to about 57 investors, in addition to $13,300 that he received from Petro for consulting fees and other payments, federal prosecutors said. After state regulators barred the sale of unregistered Petro stock, he and others "devised a plan to obtain money by gifting shares" to other investors, federal investigators said. When he sold the stock, investigators said he never mentioned that he was not licensed to sell securities, nor did he disclose the state regulatory actions or that Petro shares were unregistered.
Source: http://www.kansascity.com/2012/04/05/3538482/raymore-man-admits-to-petro-america.html

14. *April 5, Federal Bureau of Investigation* – (New York; International) **Importers charged with securities fraud.** Three principals of a company that imported paving stones from Australia were charged with conspiracy, securities fraud, and money laundering in an indictment unsealed April 5 in federal court in Central Islip, New York. The charges against the men arose from their solicitation of investor money for, and their operation of, Permapave Industries and Permapave USA. Permapave marketed porous paving stones in the United States that were manufactured in Australia. According to the indictment, the defendants issued promissory notes to investors and promised to use the proceeds to finance shipments of Permapave paving stones from Australia. The indictment and court filings charge that from 2006 to 2010, the defendants operated Permapave as a Ponzi scheme, raising approximately $26 million through false representations and paying back some investors from the investments of other investors because of the minimal revenues Permapave generated. The government's pleadings also allege that the defendants converted more than $3 million of investor funds for their personal use.
Source:
http://7thspace.com/headlines/409744/importers_charged_with_securities_fraud.html

15. *April 5, Dark Reading* – (International) **Phishers use web analytics to gauge success.** In yet another indication of cybercriminals operating more like a business, researchers have discovered a major phishing campaign that relied on Web analytics to hone its attack against a bank, Dark Reading reported April 5. Researchers at security firm RSA say a phisher targeting a specific bank in South America used a free Web analytics tool to gather statistics on how his attacks performed and details about his victims' systems. He configured it like any other Web analytics service, using embedded JavaScript code on his Web page visited by victims who fell for the phishing attack. The code records data such as the number of "hits" on the page, as well as specifics like the user's operating system and browser type. A communications specialist for RSA's FraudAction Knowledge Delivery said the attacker can glean plenty of valuable information from Web analytics: traffic trends and intelligence on the best time to send out its spam phishing run. "Using Web analytics stats, they can

get quite a bit of information: number of hits — how credible was the spam e-mail?; best time for blasting out their campaigns — night/weekends?; pages viewed per visitor — did the consumer go through the whole phishing kit?; success of a particular spam e-mailing list they've purchased; or the success of an underground spamming service they've paid for," she said.
Source: http://www.darkreading.com/insider-threat/167801100/security/client-security/232800400/phishers-use-web-analytics-to-gauge-success.html

For another story, see item **48**

[Return to top]

## Transportation Sector

16. *April 6, Hackensack Record* – (New Jersey) **Security breach forces evacuation at Newark airport.** A British man unwittingly walked past a distracted Transportation Security Agency (TSA) agent at a security checkpoint at Newark Liberty International Airport in New Jersey April 5, forcing a temporary evacuation of the terminal, authorities said. The evacuation of Terminal B lasted more than an hour as Port Authority police interviewed the man, reviewed surveillance video, and swept the terminal with bomb-sniffing dogs, said an agency spokesman. TSA officials have redoubled efforts to eliminate lax screening since a high-profile incident in 2010, when a student ducked past security to kiss his girlfriend goodbye and set off a manhunt.
Source: http://news.bostonherald.com/news/national/northeast/view/20120406security_breach_forces_evacuation_at_newark_airport/srvc=home&position=recent

17. *April 6, WNYW 5 New York* – (New York) **Bus fire blamed on mattress.** A twin-size mattress is reportedly the cause of a bizarre fire involving an MTA bus and six vehicles in the Bay Ridge area of the New York City borough of Brooklyn. Fire department officials said the bus caught fire April 5 on 7th Avenue near the Verrazano Bridge. The S53 bus dragged the mattress across the bridge. Metal springs in the mattress apparently punctured the bus' gas tank setting the bus on fire and spilling fuel. The fuel poured down the street next to parked cars and flames quickly spread to six other vehicles. The driver was able to get everyone off of the bus safely.
Source: http://www.myfoxny.com/dpp/news/bus-fire-blamed-on-mattress-brooklyn-20120406-KC

18. *April 6, Associated Press* – (Colorado; Illinois) **FAA investigating after plane emergency ignored.** The Federal Aviation Administration (FAA) is investigating after an air traffic controller was accused of ignoring a request for an emergency landing in Denver after a commercial airline pilot reported smoke in the cabin, the Associated Press reported April 6. The controller thought the call was a prank and dismissed the emergency call minutes later, according to recordings obtained by KUSA 9 Denver. The United Express plane from Peoria, Illinois, was evacuated April 3 after the plane landed at Denver International Airport. An FAA report said firefighters extinguished a

fire in the instrument panel. Airline analysts say fake calls are a problem that can originate from anyone near the airport with a radio. Controllers apparently realized the mistake when the pilot made another emergency call saying the plane had already landed and was evacuating on the runway. It was only then that fire trucks responded. One of the 21 passengers was taken to the hospital. The National Transportation Safety Board said the investigation has been turned over to the FAA.
Source: http://abcnews.go.com/US/wireStory/faa-investigating-plane-emergency-16086520#.T38P4dk-PTo

19. *April 6, Lawrence-Journal World* – (Kansas) **Two people injured in pickup-semi crash on U.S. Highway 24 in Jefferson County.** Two people suffered life-threatening injuries April 6 when a pickup truck collided with a semitrailer on U.S. Highway 24 northwest of Lawrence, Kansas. According to the Kansas Highway Patrol, a man was driving a pickup west on Highway 24, just east of Perry, when he tried to make a U-turn. His pickup crashed into a semi, a highway patrol report said. The driver was taken to the hospital by ambulance. His passenger was flown by air ambulance. The highway was closed for just over 6 hours, according to a Kansas Department of Transportation spokeswoman.
Source: http://www2.ljworld.com/news/2012/apr/06/two-people-injured-crash-semi-us-highway-24-jeffer/

[Return to top]

## Postal and Shipping Sector

20. *April 6, Merced Sun-Star* – (California) **Postal service offers $50,000 reward in Planada robbery.** The U.S. Postal Service is offering a $50,000 reward for information leading to the arrest of someone armed with a handgun who robbed one of its drivers March 30 in Planada, California. Federal investigators have not released specific details about the robbery or whether any money or property was taken. The driver, who was contracted through the U.S. Postal Service, was not hurt. Investigators from the Fresno and Stockton offices of the U.S. Postal Inspection Service are working with state and local authorities in the investigation.
Source: http://www.mercedsunstar.com/2012/04/06/2298525/postal-service-offers-50000-reward.html

[Return to top]

## Agriculture and Food Sector

21. *April 6, Food Safety News* – (International) **BC issues warning about pomeberry frozen berries.** Eight cases of hepatitis A over the past 2 months in British Columbia may be linked to frozen berries, the British Columbia Center for Disease Control (BCCDC) said April 5. It warned consumers not to eat Pomeberry Blend frozen berries manufactured by Western Family. The blend, which was distributed through Save-On-Foods and Overwaitea, contains frozen pomegranate seeds, blueberries, strawberries,

and cherries. According to the news release, five of the eight people ill with the virus are known to have consumed the Pomeberry product. Although there is no direct link yet, the BC health authorities suggest as a precaution, individuals who have the Pomeberry Blend product in their refrigerator or freezer should not to consume it and should discard it. At this time, the BCCDC thinks the overall risk to the public is very low, and it is not recommending that people who have consumed the product should receive vaccine.
Source: http://www.foodsafetynews.com/2012/04/bc-issues-warning-about-pomeberry-frozen-berries/

22. *April 5, Food Safety News* – (International) **Cryptosporidium spurs parsley recall in Canada.** The Canadian Food Inspection Agency (CFIA) is warning the public not to consume Boskovich brand fresh parsley imported from the U.S. because it may contain Cryptosporidium, Food Safety News reported April 5. The affected product was sold only March 19 from one store, Canada Safeway in Saskatoon, Saskatchewan. The product was sold in bunches enclosed with a band indicating the Boskovich brand and Product of USA. Food contaminated with Cryptosporidium hominis may not look or smell spoiled. Consumption of food contaminated with these protozoans may cause cryptosporidiosis, a foodborne illness.
Source: http://www.foodsafetynews.com/2012/04/cryptosporidium-prompts-parsley-recall-in-canada/

23. *April 5, Food Safety News* – (New York; Ohio) **Allergen alert: Coconut candy with milk.** Fung Shing International Corp. of Maspeth, New York, is recalling Star Light Coconut Candy because it contains milk not declared on the label, Food Safety News reported April 5. Routine sampling by New York State Department of Agriculture and Markets Food inspectors and subsequent lab analysis revealed the presence of milk in the product. The recalled Star Light Coconut Candy Keo Dua is imported from Vietnam. The recalled candy was sold in New York and Ohio.
Source: http://www.foodsafetynews.com/2012/04/allergen-alert-coconut-candy-with-milk/

24. *April 5, Food Safety News* – (International) **Salmonella concern spurs tahini recall in Canada.** The Canadian Food Inspection Agency is warning the public not to consume Ayyam Zaman brand Extra Fine Tahina as it may be contaminated with Salmonella, Food Safety News reported April 5. The affected product, Ayyam Zaman brand Extra Fine Tahina, is sold in 400 gram packages. This product is known to have been distributed in Ontario and may have been distributed in other provinces as well.
Source: http://www.foodsafetynews.com/2012/04/salmonella-concern-spurs-tahini-recall-in-canada/

[Return to top]

## Water Sector

25. *April 6, Pottsville Republican Herald* – (Pennsylvania) **Boil water order issued for Girardville.** Due to an April 5 water main break, Aqua America issued a precautionary water boil order for Girardville, Pennsylvania, until further notice. According to the utility's Web site, a contractor hit a transmission main, leaving some areas temporarily without water. Aqua planned to flush the distribution system, collect water samples, and notify customers when they can stop boiling their water.
Source: http://republicanherald.com/boil-water-order-issued-for-girardville-1.1296286

26. *April 5, Associated Press* – (Iowa) **1 injured in blast at Dubuque wastewater plant.** Police in Dubuque, Iowa, said one person was injured in an explosion and fire at the city's wastewater treatment plant April 6. The Dubuque Telegraph Herald reported the explosion happened in one of the plant's incinerators. Firefighters and emergency crews from the Dubuque Fire Department responded to the scene. One employee was transported to an area hospital. The water treatment plant is in the midst of a $64 million facility upgrade. Damage from the fire was centered in an older part of the plant and was not expected to hinder the facility's operation. Fire officials were investigating the cause of the fire.
Source: http://qctimes.com/news/state-and-regional/iowa/injured-in-blast-at-dubuque-wastewater-plant/article_1ebb793e-7ae5-50ba-aad4-60e214283c4b.html#ixzz1rGg49QgX

For another story, see item **39**

[Return to top]

## Public Health and Healthcare Sector

27. *April 6, Psych Central News* – (National) **ADHD drug shortage to end soon.** After months of Americans being unable to fill their drug prescriptions for medications that are commonly used to treat attention deficit hyperactivity disorder (ADHD), the U.S. Food and Drug Administration said April 5 the shortages are expected to end before May. Many ADHD medications, such as Adderall, have been in short supply since 2011.
Source: http://psychcentral.com/news/2012/04/06/adhd-drug-shortage-to-end-soon/37059.html

28. *April 6, Associated Press* – (Maryland) **Md. health officials warn against cold med Baczol.** Maryland health officials are warning against using an unapproved medicine called Baczol, which has been found in some Maryland stores, the Associated Press reported April 6. The Department of Health and Mental Hygiene says the product, often marketed as a pediatric cold medicine, is ineffective against some conditions for which it is purchased and contains an antibiotic that requires a prescription. The U.S. Food and Drug Administration has issued an import alert for the medication, sold under the names Baczol, Pediatric Baczol, or Baczol Antigripal.
Source: http://www.wtop.com/?nid=740&sid=2817252

29. *April 6, Associated Press* – (Iowa) **Polk County warns parents about whooping cough.** Polk County, Iowa health authorities sent letters to parents at three schools, warning them about cases of whooping cough, the Associated Press reported April 6. The county Health Department said at least 11 cases of whopping cough have been confirmed. The cases were reported in students at Weeks Middle School, Lincoln High School, and Lincoln South. The officials say the number of cases is not especially high, but the concentration of cases and the highly contagious nature of whooping cough spurred the warning.
Source: http://www.kttc.com/story/17350974/polk-county-warns-parents-about-whooping-cough

30. *April 4, Iowa City Press-Citizen* – (Iowa) **Mercy nurse charged with stealing patients' meds.** A former Mercy Hospital nurse in Iowa City, Iowa, was charged with more than a dozen counts of stealing prescription drugs from the hospital's drug dispensing machine, the Iowa City Press-Citizen reported April 4. She allegedly withdrew medication from the hospital's Pyxis drug dispensing machine under various patients' names on 37 different occasions between September 2009 and January 2010, according to police reports. Police records state she would withdraw morphine and hydromorphone for various patients that were under her care and did not document the waste amount as required. She admitted to police during an interview that she would "abuse medication when she could get away with it." In addition, the portions of the dispensed medications for her personal use were billed to the patients by the hospital.
Source: http://www.press-citizen.com/article/20120405/NEWS01/304050017/Mercy-nurse-charged-stealing-patients-meds?odyssey=nav|head

[Return to top]

## Government Facilities Sector

31. *April 6, NewsCore* – (California) **Oakland university shooter was hunting staff member refused to refund his tuition, police say.** The man accused of slaughtering seven people at Oikos University in Oakland, California, was hoping to find and kill an administrator who no longer works at the school, police said April 5. The suspect — who is reported to have confessed to the April 2 killing spree — was angry that the woman who refused him a full refund of his $6,000 tuition fees when he dropped out of his nursing classes late in 2011, the Oakland Tribune reported. Police said the woman left the school soon after the suspect. When he failed to find the woman, the suspect instead killed six students and a receptionist with a semiautomatic handgun. He reportedly also wounded three other people, before stealing a victim's car and driving to nearby supermarket where he admitted his crimes to staff and was arrested, officials said. He is charged with seven counts of murder and related offenses.
Source: http://www.foxnews.com/us/2012/04/06/oakland-university-shooter-was-hunting-staff-member-refused-to-refund-his/

32. *April 5, WESA 90.5 FM Pittsburgh* – (Pennsylvania) **More bomb threats at the University of Pittsburgh.** The University of Pittsburgh evacuated four buildings April

5 after receiving a bomb threat aimed at the Cathedral of Learning, the Chevron Science Building, Frick Fine Arts Building, and Posvar Hall. Over the last 3 weeks there have been 23 threats, but no explosives have been found. The university's vice chancellor for public affairs said the investigation continues into these threats, and a $50,000 reward is now being offered for information. The bomb threats have been made against several buildings on campus, and the university is very concerned about the psychological effect of these threats. He added that even though the threats so far have turned out to be hoaxes, they must be taken very seriously. Pittsburgh police have enlisted the help of the FBI and handwriting experts while trying to solve the case. They have said that they intend to prosecute anyone connected to the threats to the "fullest extent possible" under federal and state laws.
Source: http://www.essentialpublicradio.org/story/2012-04-05/more-bomb-threats-university-pittsburgh-10685

33. *April 5, Orlando Sentinel* – (Florida) **Fruitland Park students return to classrooms after fifth-grader brings mortar to school.** Students at Fruitland Park Elementary in Fruitland Park, Florida, were evacuated to a nearby church for almost 4 hours April 5 after administrators learned a student brought a mortar to school in his backpack, officials said. A fifth-grader brought the mortar to school to show his friends, a district spokesman said. Fruitland Park Police and the Lake County Sheriff's Office Bomb Squad responded to the scene. A sheriff's lieutenant said it did not appear the mortar was active, but the bomb squad brought in a robot to remove it from the campus.
Source: http://www.sun-sentinel.com/news/local/breakingnews/os-fruitland-park-school-evacuated-mortar-20120405,0,550204.story

34. *April 4, KDKA 2 Pittsburgh* – (Pennsylvania) **Shaler Elementary School closed after air duct collapse.** Several students and teachers from Shaler Area Elementary School in Shaler, Pennsylvania, were recovering April 4 after some ductwork fell from the ceiling of the school during a crowded lunch period April 3. As repairs and inspections are made at the school, the cafeteria will remain closed for the rest of the school year. Shaler Area Elementary School was closed April 4 after a dozen children and teachers were injured when an air duct in the cafeteria unhinged and fell from the ceiling during fourth grade lunch period. The school superintendent shut down two gymnasiums in another school, saying that the same company responsible for the 2007 renovations at the elementary school also did work at the high school. An expert from the district attorney's office was helping with the investigation, and the area was being treated as a crime scene.
Source: http://pittsburgh.cbslocal.com/2012/04/04/shaler-elementary-school-closed-after-air-duct-collapse/

35. *April 2, Fierce Government IT* – (National) **Internet voting not ready for elections, says DHS official.** Unresolved technological problems means Internet voting should not yet be deployed to U.S. elections, a Homeland Security Department cybersecurity official told a conference of election officials and watchdogs. "It's definitely premature to deploy Internet voting in real elections," said the official, speaking before the Election Verification Network conference in Santa Fe, New Mexico, March 29. "The

security infrastructure around Internet voting is both immature and under-resourced," he told the audience, citing National Institute of Standards and Technology (NIST) internal reports that summarize technical research on particular subjects. When it comes to end-to-end cryptographic voting techniques, the NIST report states that they "are largely still an academic effort."
Source: http://www.fiercegovernmentit.com/story/internet-voting-not-ready-elections-says-dhs-official/2012-04-02

For another story, see item **29**

[Return to top]

## Emergency Services Sector

See items **45** and **51**

[Return to top]

## Information Technology Sector

36. *April 6, H Security* – (International) **Google Chrome fixes seven high-risk vulnerabilities.** Google has announced updates to the Stable and Beta channels of their Chrome browser, fixing several bugs and 12 security vulnerabilities. Seven of the 12 security fixes were classed as high-risk problems and Google paid a total of $6,000 to the researchers who discovered the bugs. The seven high risk vulnerabilities are bugs that left several Chrome components open to being exploited by using memory after it had been freed. The Chrome developers have also fixed several cross-origin problems and two issues where the browser could be exploited to read from memory where it should not.
Source: http://www.h-online.com/security/news/item/Google-Chrome-fixes-seven-high-risk-vulnerabilities-1517293.html

37. *April 6, IDG News Service* – (International) **Sophos takes down partner portal after signs of hacking.** Security firm Sophos has taken its partner portal offline and will reset every user's password after it found signs of a potential security breach on the server hosting it during a routine security check April 3. "Two unauthorized programs were found on the server, and our preliminary investigations indicate that these were designed to allow unauthorized remote access to information," Sophos said in a security alert posted on its Web site. Sophos could not establish if the data stored in the Web site's database — which includes partners' names and business addresses, e-mail addresses, contact details, and hashed passwords — had been stolen. However, it decided to proceed under the assumption that it had. The Web site will be restored after the security audit is completed and the problem is remediated. The company advised its partners to also change their passwords on other Web sites where they might have used them, and to be on alert for potential phishing e-mails that claim to originate from Sophos.

Source: http://www.computerworld.com/s/article/9225921/Sophos_takes_down_partner_portal_after_signs_of_hacking

38. *April 5, Microsoft Certified Professional Magazine* – (International) **Six bulletin items announced ahead of April's Microsoft security update.** Microsoft will release six bulletin items in its April security update, according to the Microsoft Security Bulletin Advance Notification. The monthly patch will feature four "critical" items and two "important" bulletins. All four of the critical bulletins will address remote code execution vulnerabilities in Windows, Internet Explorer, Microsoft .NET Framework, Microsoft Office, Microsoft SQL Server, Microsoft Server Software, and Microsoft Developer Tools. As for the two important bulletin items, the first addresses an information disclosure flaw in Microsoft Forefront United Access Gateway, and the second targets an additional remote code execution hole in Microsoft Office. After March's alleged leak of RCP code, a security researcher at Rapid7 discussed the possible tightening of security procedures when it comes to releasing security information to Microsoft partners.
Source: http://mcpmag.com/articles/2012/04/05/six-bulletin-items-announced.aspx

39. *April 4, Network World* – (National) **DHS: America's water and power utilities under daily cyber-attack.** America's water and energy utilities face constant cyber-espionage and denial-of-service attacks against industrial-control systems, according to the team of specialists from the U.S. Department of Homeland Security (DHS) who are called to investigate the worst cyber-related incidents at these utilities, Network World reported April 4. Out of the 17 fly-away trips taken in 2011 by DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to assist utilities in network and forensics analysis, 7 of the security incidents originated as spear-phishing attacks via e-mail against utility personnel. An ICS-CERT leader said 11 of the 17 incidents were very "sophisticated," signaling a well-organized "threat actor." She said DHS believes that in 12 of the 17 cases, if only the compromised utility had been able to practice the most basic type of network security for corporate and industrial control systems, they would likely have detected or fended off the attack. One of the basic problems observed at utilities is that "a lot of folks are using older systems previously not connected to the Internet," she said. Another ICS-CERT leader said the count of "incident tickets" related to reported incidents at water and power-generating utilities is going up. While only 9 incidents were reported in 2009, in 2011 this grew to 198 incident tickets. Just over 40 percent came from water-sector utilities, with the rest from various energy, nuclear energy, and chemical providers. He said in many cases the attacks do not seem to be coming directly through the Internet via Internet Service Providers, for example, but are often traced to outside companies that provide services to the attacked utilities, raising the question of compromises there.
Source: http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html?page=1

For more stories, see items **15**, **44**, and **48**

## 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

40. *April 6, WYMT 12 Hazard* – (Kentucky) **Phone service knocked out again in Letcher Co.** Copper thieves struck again in Letcher County, Kentucky, WYMT 12 Hazard reported April 6. The thieves took 200 feet of copper wiring, leaving many homes and businesses around the Isom area without phone service for most of the day April 5. Kentucky State Police confirmed that this outage was the result of copper thieves.
Source: http://www.wkyt.com/wymt/home/headlines/Phone_service_out_again_in_Letcher_Co_146354755.html

41. *April 5, al.com* – (Alabama) **Central Alabama weather radio outage fixed.** As severe thunderstorms threatened the state, forecasters from the National Weather Service (NWS) office in Birmingham, Alabama, warned residents April 5 their weather alert radios might not receive alerts, but the NWS reported the problem has been identified and resolved. The outages — reported in Montgomery and Anniston but possibly occurring elsewhere — meant some weather radios did not sound when a watch or warning was issued. Weather service technicians worked to identify and correct the problem, according to the NWS. The outage was reportedly caused by a hardware failure.
Source: http://blog.al.com/montgomery/2012/04/central_alabama_weather_radios.html

42. *April 5, Vancouver Columbian* – (Washington) **Software glitch knocks out Internet in east county.** A rare software-related problem triggered an outage of Internet access to some 1,800 Frontier Communications customers in Camas and Washougal, Washington, that began the evening of April 4 and extended into mid-day April 5, according to the utility's general manager. Internet service has been restored to all Frontier customers, he said. The outage affected about half of the utility's Washougal and Camas customers with Internet services, primarily residences and small businesses. The problem emerged in software used in some of Frontier's newest switches and routers, the manager said.
Source: http://www.columbian.com/news/2012/apr/05/software-glitch-knocks-out-internet-east-county/

43. *April 5, Wausau Daily Herald* – (Wisconsin) **Charter Internet service out for some Wausau-area customers.** Some Wausau, Wisconsin-area residents were experiencing an Internet outage April 5 that was expected to last for several hours. A company

supervisor said at 9:15 p.m. that a "fluctuating signal" was to blame for the outage in the Wausau area and other parts of the state, according to a company supervisor at Charter Communications. A total of 1,200 customers across the state were affected, the supervisor said. The estimated time for repairs was 3 to 4 hours, according to the supervisor.
Source:
http://www.wausaudailyherald.com/article/20120405/WDH0101/120405126/Charter-Internet-service-out-some-Wausau-area-customers?odyssey=mod|newswell|text|FRONTPAGE|s

44. *April 5, Help Net Security* – (National; International) **Fake AT&T wireless bill links to malware.** Large outbreaks of phony AT&T wireless e-mails were distributed in the last 2 days, Commtouch said April 5. The e-mails describe very large balances ($943), that are sure to get aggravated customers clicking on the included links. Every link in the e-mail leads to a different compromised site with malware hidden inside. The pattern is: legitimate domain / recurring set of random letters / index.html. The index.html file tries to exploit at least the following known vulnerabilities: Libtiff integer overflow in Adobe Reader and Acrobat — CVE-2010-0188; and Help Center URL Validation Vulnerability — CVE-2010-1885.
Source: http://www.net-security.org/malware_news.php?id=2057

[Return to top]

## Commercial Facilities Sector

45. *April 6, Associated Press* – (Texas) **Police: Officer killed at Texas Walmart, suspect arrested.** A police officer was shot and killed April 6 at a Walmart in Austin, Texas, and a suspect was in custody, police said. The officer was responding to a call about a drunk man inside the store. The suspect attacked the officer as soon as he arrived at the store. "The suspect produced a semi-automatic pistol and shot the officer at point blank range," Austin's Police chief said. The wounded officer was able to call for help using his police radio, he added. Two Walmart employees tackled and held the suspect and locked down the store until another police officer arrived to arrest him. Store video captured the entire incident.
Source: http://www.foxnews.com/us/2012/04/06/officer-fatally-shot-at-walmart-in-texas/

46. *April 6, Long Beach Press-Telegram* – (California) **Stun grenades force evacuation of stores near Redondo Beach mall.** Two active-duty Marines who caused the evacuation of a parking lot and several stores near a Redondo Beach, California shopping center were in custody April 6 after non-lethal artillery simulators were found in a pickup truck they were driving, police said. Officers found their pickup in the parking lot of a furniture store adjacent to the South Bay Galleria shopping center, and detained the two men, who were standing next to the vehicle. Officers cordoned off the parking lot and evacuated the furniture store and two adjacent stores while the bomb squad was called. About 3 hours after the pickup was found, the bomb squad recovered

10 “military artillery simulator training aids” from the vehicle, a police official said. The two men were later taken into custody by Naval Criminal Investigative Services agents.
Source: http://www.presstelegram.com/breakingnews/ci_20340028/stun-grenades-force-evacuation-stores-near-redondo-beach

47. *April 6, Raycom News Network* – (Virginia) **Pilots delayed jet crash to avoid school.** An F/A-18D Hornet Navy fighter jet crashed into an apartment complex near Virginia Beach, Virgina, sending fuel and debris flying and erupting into flames April 6. Both crew members — who ejected at the very last moment to avoid a nearby school — and five civilians on the ground were treated at local hospitals. An eyewitness to the plane crash said that within 200 or 300 yards of where the plane crashed, the aircraft emptied its jet fuel, with its nose up, and crashed into a building at the Mayfair Mews Apartments. At least five buildings were heavily damaged. The Associated Press reported the fire was out, and crews were going through the buildings to check for anyone who may have been injured. One of the pilots was found on the ground, still strapped to his seat, in shock, according to a witness. The crash site is just north of Oceana Naval Air Station in Virginia, where the crew is based.
Source: http://www.wtvm.com/story/17351737/f-18-crashes-near-virginia-beach

48. *April 5, Seattle Post Intelligencer* – (Washington) **Final defendant admits to Seattle-area Wi-Fi hacking scheme.** The final defendant in a hacking and burglary scheme that saw more than 40 Seattle-area businesses attacked pleaded guilty to a host of federal crimes. The defendant pleaded guilty to stealing personal information of employees of at least 13 businesses by infiltrating companies’ Wi-Fi networks between April 2008 and December 2010, when he and a second man were arrested. He and two other men then used that information to obtain credit cards, while also rerouting company checks to themselves. Investigators ultimately discovered the hackers were finding networks to target by “wardriving” -– driving around with a high-strength Wi-Fi receiver inside a car to search for networks that can be penetrated.
Source: http://www.seattlepi.com/local/article/Final-defendant-admits-to-Seattle-area-Wi-Fi-3461908.php

49. *April 5, South Florida Sun-Sentinel* – (Florida) **Serial arson suspect arrested in Sunrise.** A 52-year-old Sunrise, Florida man accused of setting more than 20 fires in and around the apartment complex where he lives was arrested April 4, according to Sunrise Police. The suspect was charged with burglary and arson after he broke into a neighbor’s apartment and set his mattress on fire, police said. He was also suspected of setting 21 other fires in several neighboring apartment buildings and in dumpsters near several area businesses, police said.
Source: http://articles.sun-sentinel.com/2012-04-05/news/fl-sunrise-arsonist-arrested-20120405_1_serial-arson-sunrise-man-fires

[Return to top]

## National Monuments and Icons Sector

50. *April 6, WCAU 10 Philadelphia* – (New Jersey) **Wildfires char NJ's preserved land.** Two wildfires were scorching land inside the Winslow Wildlife Management Area in southern New Jersey, WCAU 10 Philadelphia reported April 6. One fire covered about 100 acres and was not under control as of April 6. That fire was closest to the A.C. Expressway. Firefighters had a better handle on the smaller fire, which was spread across approximately 25 acres. That area in Winslow Township is the second largest contiguous piece of preserved land in Camden County. The State's Forest Fire Service Web site reported April 6 that the fire danger for all of Central and South Jersey was at the "Very High" stage, which is the second highest level of alert.
Source: http://www.nbcphiladelphia.com/news/local/Large-Brush-Fires-New-Jersey-Winslow-Wildlife-146422275.html

51. *April 5, Associated Press* – (Colorado) **Report: Colo. wildfire a deadly cascade of missteps.** New documents released the week of April 2 show that a deadly cascade of missteps combined with the vagaries of wind and fire to produce another tragedy in the Rocky Mountains, according to an April 5 report from the Associated Press. The Colorado State Forest Service conducted a 50-acre prescribed burn on March 22, part of a normal plan to consume fuel in the foothills southwest of Denver. Once the fire was out, crews patrolled the perimeter daily. March 26, they spotted an ember blown across the perimeter and lighting grass. In all their methodical planning, they had not asked for real-time weather forecasts that would have predicted vicious, swirling winds. The 6-square-mile blaze killed three people, destroyed dozens of homes near Conifer, and raised questions about what could have been done to contain the human and material losses. Volunteer firemen responding to the first reports of smoke could not talk to the state crew because it used a different radio frequency. Dispatchers, too, were in the dark, reassuring some frightened residents as the smoke and winds gathered that events were under control. When authorities realized more than 3 hours later that, in fact, nothing was under control, they sent out waves of emergency evacuation telephone calls — some of which reached no one, while others went to out-of-state numbers. Some early callers died in the inferno. Harried dispatchers hung up on other callers, too overwhelmed to respond. The first evacuation orders did not go out until at least 3 hours after the embers ignited. The family of a deceased victim said the victim did not receive an evacuation call because her property was listed at the wrong address. Some residents said they never knew about the controlled burn, despite policies mandating the public be informed well in advance. Ultimately, residents of some 900 homes were evacuated amid rapidly changing weather conditions typical of Colorado's foothills and mountains.
Source: http://www.firehouse.com/news/10689261/report-colo-wildfire-a-deadly-cascade-of-missteps

[Return to top]

## Dams Sector

52. *April 6, Billings Gazzette* – (Montana) **Corps plans Fort Peck spillway test.** The U.S. Army Corps of Engineers plans to release 3,000 to 30,000 cubic feet per second (cfs) of

water through the Fort Peck Dam spillway in Montana during the summer of 2012 to ensure it is performing properly after 2011's year of high water. The test will help engineers determine whether a subdrain system that relieves pressure beneath the spillway is functioning. "We have concerns about those drains working properly," said the Corps' project manager. The test will take place over 4 days and would raise the water level directly downstream of the dam up to 4.7 feet with the highest test releases of 30,000 cfs. That rise would quickly dissipate the farther downstream the water travels, with the river near Wolf Point rising 1.7 feet. Near Culbertson, the river would rise 1.1 feet. Officials said the drop in the lake level would be insignificant. The public would be given a minimum of 30 days advance notice of the test dates.
Source: http://billingsgazette.com/news/state-and-regional/montana/corps-plans-fort-peck-spillway-test/article_83fac5c8-af16-53df-a6d2-c6f4c0a0ddb2.html

[Return to top]


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

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

### Contact Information

| | |
|---|---|
| Content and Suggestions: | Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267 |
| Subscribe to the Distribution List: | Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes. |
| Removal from Distribution List: | Send mail to support@govdelivery.com. |

### Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

### Department of Homeland Security Disclaimer