



Homeland
Security

Daily Open Source Infrastructure Report

16 April 2012

Top Stories

- Nearly 61 percent of 48 states are in abnormally dry or drought conditions, according to the U.S. Drought Monitor. These conditions have led to numerous wildfires and put many agricultural crops at risk. – *USA Today* (See item [15](#))
- Two U.S. Coast Guard members were found shot to death while at work in Kodiak Island, Alaska, in what officials said appeared to be a double homicide. – *Associated Press* (See item [29](#))
- Oracle plans to release 88 patches April 17, including many that fix vulnerabilities that allow remote access to the Oracle database without a username and password. – *IDG News Service* (See item [38](#))
- Two reports found that scaffolding that collapsed and killed seven people during the Indiana State Fair in 2011 was subpar. The reports also indicate the fair's commission did not have adequate emergency planning in place. – *CNN* (See item [45](#))

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 13, Contra Costa Times* – (California) **Fire at Rodeo refinery causes scare, hazmat finds no harmful release.** A fire that broke out at the ConocoPhillips refinery in Rodeo, California, April 13 caused a scare that subsided after a HAZMAT crew found no harmful chemicals were released, officials said. The fire was reported about 1 a.m. at the sulfur recovery unit of the refinery, prompting the issuing of a precautionary health advisory urging residents living near the compound to stay indoors in case particulates were released. An on-site fire-response team quickly put out the blaze. Specialists from the Contra Costa Hazardous Materials Team went to the site and tested the air and found no traces of hydrogen sulfide or sulfur dioxide, the agency director said . A cause for the fire or the extent of damage was not immediately known. Source: http://www.mercurynews.com/breaking-news/ci_20388694/health-advisory-rodeo-lifter-after-fire-extinguished-at
2. *April 12, San Gabriel Valley Tribune* – (California) **Investigator: Improper maintenance led to tanker-truck fire that damaged Montebello freeway bridge.** The California Highway Patrol (CHP) is pursuing charges against the company that owned a tanker truck that burst into flames on the 60 Freeway in Montebello, December 2011, severely damaging an overpass, the San Gabriel Valley Tribune reported April 12. A CHP investigator found the fire was caused by improper maintenance of the truck. The Paramount Boulevard bridge over the 60 Freeway was severely damaged when the truck, carrying 9,000 gallons of gasoline, caught fire. The driver fled from the burning truck, which then rolled to a stop under the bridge. The intense heat compromised the integrity of the bridge’s concrete and steel, forcing the California Department of Transportation (Caltrans) to have it demolished. The cost of reconstruction is expected to be \$40 million. An investigation suggested the truck’s driveshaft had not been not properly maintained, causing it to come loose. The investigator found the driveshaft swung around and punctured the gas tank. Sparks caused by it scraping on the ground ignited the leaking fuel. The final results of the investigation could determine whether the truck’s owner — Cool Transports of Bloomington — is on the hook for bridge replacement costs, Caltrans officials said. Source: http://www.sgvtribune.com/news/ci_20386275/investigator-improper-maintenance-led-tanker-truck-fire-that

[\[Return to top\]](#)

Chemical Industry Sector

3. *April 13, Salt Lake Tribune* – (Utah) **Semi crash causes SR 44 closure in Daggett County.** One person was injured April 12 after a tractor-trailer carrying a bleach product rolled about 10 miles south of Manila in Daggett County, Utah. A Utah High Patrol corporal said the semi trailer was driving on State Route 44 when the truck rolled

onto its top. He said the truck was carrying about 12 barrels filled with sodium chlorite, a bleach solution. He said all of the barrels were damaged. The driver was injured and was air-lifted to a hospital in serious condition. The driver told troopers he lost control of the vehicle while taking evasive action to miss an animal. The wreck prompted officials to close the roadway in both directions for less than an hour while they cleaned up the spill, the corporal said.

Source: <http://www.sltrib.com/sltrib/news/53903342-78/johnson-crash-barrels-bleach.html.csp>

4. *April 12, Associated Press* – (West Virginia; Ohio) **Medical panel appointed for W.Va. C8 case.** A panel of physicians has been selected to determine the extent of medical monitoring for residents exposed to a chemical while living near a DuPont plant near Parkersburg, West Virginia. DuPont and attorneys for Mid-Ohio Valley residents who settled a class-action lawsuit against the company in 2005 announced the three-member panel April 12. The panel was named as part of the settlement of the lawsuit that claimed perfluorooctanoic acid, or C8, contaminated water supplies in Ohio and West Virginia. DuPont uses C8 at its Washington Works plant.
Source: <http://www.wtrf.com/story/17401788/medical-panel-appointed-for-wva-c8-case>
5. *April 12, Charlotte Observer* – (North Carolina) **1 injured in Caldwell chemical plant fire.** One worker was hurt and hundreds evacuated April 12 when a fire broke out a Caldwell County, North Carolina chemical plant. The fire occurred at RPM Wood Finishes Group in Hudson. The plant makes dyes, lacquers, and other coatings for furniture. A RPM spokesman said a flash fire erupted in a tank in the paints and coatings production building. The 250 employees working at the time were evacuated, and the fire was contained. The injured employee was taken to a hospital. Hudson fire officials said the fire was under control in 30 minutes. They said no hazardous materials were released. U.S. 321 was closed for a few hours as emergency crews responded to the fire.
Source: <http://www.charlotteobserver.com/2012/04/12/3169105/fire-erupts-at-caldwell-county.html>

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

6. *April 12, Associated Press* – (California) **More wear found on tubes at ailing Cal nuke plant.** Southern California Edison announced April 12 that more unusual wear was found on tubing that carries radioactive water at both of San Onofre Nuclear Generating Station's reactors, the latest disclosure in a mystery involving the plant's steam generators. Investigators at the plant in San Diego County, California, found additional damage on tubes in its Unit 2 generators that was similar to degradation in its sister reactor, Unit 3, though at a lower level. The new findings showed "all of the generators are exhibiting the same kind of wear, though the wear in unit 3 is more excessive than in Unit 2," a Nuclear Regulatory Commission spokesman said. The plant has been shut down for more than 2 months while federal regulators and company

officials try to find out why tubing designed to withstand many years of use under high pressure has eroded at an unusual rate.

Source: <http://www.cbsatlanta.com/story/17396119/more-wear-found-on-tubes-at-ailing-cal-nuke-plant>

[\[Return to top\]](#)

Critical Manufacturing Sector

Nothing to report

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Banking and Finance Sector

7. *April 13, Salt Lake Tribune* – (Utah) **Utah couple charged with interfering with IRS.** A Taylorsville, Utah couple who have not filed tax returns since the 1990s has been indicted on charges that include an allegation they placed false liens against top tax officials, trying to collect nearly \$2 million, the Salt Lake Tribune reported April 13. The couple is facing five counts of impeding the Internal Revenue Service (IRS) and filing false liens or encumbrances against government officials. The indictment alleges that starting in December 2010, the couple started filing documents with county clerks directed at high-ranking officials within the U.S. Department of the Treasury and mailing demands for money to the private residence of a Treasury official. The woman filed a false lien against an IRS commissioner and the comptroller of the currency for \$949,471 at the Salt Lake County Recorder’s Office, the indictment alleges. The couple also mailed multiple “Demand for Payment” documents to the residence of the IRS commissioner in 2011 demanding payments of \$949,471 and \$984,661, court documents say. The couple was arrested April 10 and pleaded not guilty in federal court April 11.

Source: <http://www.sltrib.com/sltrib/money/53904195-79/irs-couple-filed-tax.html.csp>

8. *April 12, WPVI 6 Philadelphia* – (Pennsylvania; Delaware) **Police: Woman bank bandit, accomplice arrested in Delaware.** Delaware State Police arrested a woman they say robbed four Wilmington, Delaware-area banks over the last 3 weeks. The woman and an accomplice were arrested April 11 and charged with robbery, conspiracy, and related offenses in connection with four holdups. Police say the latest robbery occurred April 11 at about 11:52 a.m. as a female suspect entered a PNC Bank located inside a Super G Food Market in Wilmington. She approached the teller and presented a demand note for money, implying she had a gun. The teller complied and the suspect fled the bank on foot with an undisclosed amount of cash. A short time

later, a Delaware State trooper spotted a car matching the description of a suspect vehicle observed leaving the area of the robbery. Troopers conducted a vehicle stop. The occupants of the vehicle were identified as the suspects. Both were arrested. The woman was linked to three other holdups and charged. The accomplice was charged with the April 11 holdup.

Source: <http://abclocal.go.com/wpvi/story?section=news/local&id=8618377>

9. *April 12, Federal Bureau of Investigation* – (California) **Former chief financial officer of Irvine technology firm indicted in embezzlement scheme and returned to California today.** A federal grand jury returned an indictment April 11 that charges the former chief financial officer of an Irvine, California-based technology company with a fraud scheme to embezzle about \$16 million from his employer, a U.S. attorney and the FBI announced. The defendant has remained in federal custody since he was arrested in March upon entering the United States through New York’s John F. Kennedy International Airport. According to a criminal complaint filed March 30, representatives for an Irvine-based company, Trustin Technology, contacted law enforcement with suspicions the man had embezzled funds prior to resigning from the company in February 2012. The complaint alleged company executives had approached him with growing concerns about the firm’s finances earlier in 2012 but were advised by the man that delinquent customer payments had caused a cash flow shortage. When he resigned, an analysis of Trustin’s accounting records revealed he had been diverting the company’s money to his personal bank accounts, the complaint said. According to the indictment, he had been misappropriating Trustin customer payments since at least 2009. He manipulated balance sheets to make it appear customer payments were directed to the company’s accounts, when they were actually controlled by the defendant. The indictment alleges he caused losses to Trustin Inc. in excess of \$16 million.

Source: <http://www.fbi.gov/losangeles/press-releases/2012/former-chief-financial-officer-of-irvine-technology-firm-indicted-in-embezzlement-scheme-and-returned-to-california-today>

10. *April 12, U.S. Commodity Futures Trading Commission* – (Illinois; National) **CFTC orders Rosenthal Collins Group, LLC, a registered futures commission merchant, to pay more than \$2.5 million for supervision and record-production violations.** The U.S. Commodity Futures Trading Commission (CFTC) announced April 12 the filing and simultaneous settlement of charges against Rosenthal Collins Group, LLC (RCG), a Chicago-based registered futures commission merchant, for failing to diligently supervise the handling by its officers, employees, and agents of an account held at RCG in the name of Money Market Alternative, LP (MMA). An employee used the MMA account in a multi-million dollar Ponzi scheme. According to the CFTC’s order, from April 1, 2006 until April 29, 2009, RCG failed to diligently supervise the handling of the MMA account. Specifically, the order finds RCG failed to follow its own compliance procedures that impose continuing duties to “know” its customers and detect and report “any suspicious money transfers, non-economic transactions, and other activity outside of the ordinary course of business.” For example, MMA stated in its account opening documents that it had a net worth of \$300,000 and an annual income of \$45,000, but deposits in the MMA account at RCG

exceeded \$2 million in 2006, \$3 million in 2007, and \$14 million in 2008. The MMA account also experienced losses of more than \$17 million and generated \$921,260.90 to RCG in gross commissions and fees. The order further finds RCG failed to investigate and report years of excessive wire activity relating to the MMA account. The order requires RCG to pay a \$1.6 million civil monetary penalty, and to disgorge \$921,260.90 to the scheme's victims.

Source: <http://www.cftc.gov/PressRoom/PressReleases/pr6230-12>

For more stories, see items [26](#) and [44](#)

[\[Return to top\]](#)

Transportation Sector

11. *April 13, Associated Press* – (National; International) **Lightning forces United flight return to airport.** An official at San Francisco International Airport in San Francisco said lightning hit a United Airlines flight, April 12, forcing the plane to return to the airport. A duty manager said the plane landed safely and there were no injuries to anyone. A spokeswoman from United said the Boeing 777 carrying 258 passengers was en route to London, England. Maintenance workers were inspecting the aircraft. Passengers were expected to fly to London April 13.

Source: http://www.mercurynews.com/breaking-news/ci_20388740/lightning-forces-united-flight-return-airport

12. *April 12, WBIR 10 Knoxville* – (Tennessee) **Loaded gun found in passenger's bag at McGhee Tyson Airport.** A Transportation Security Administration (TSA) agent found a loaded gun at the security checkpoint at McGhee Tyson Airport April 11 in Knoxville, Tennessee. Airport police were alerted, confiscated the gun, and cited the passenger. The TSA said the incident was the fifth firearm discovery at the airport's checkpoint so far this year.

Source: <http://www.wbir.com/news/article/215846/2/Loaded-gun-found-in-passengers-bag-at-McGhee-Tyson-Airport?odyssey=tab|topnews|bc|large>

For more stories, see items [2](#), [3](#), [5](#), and [43](#)

[\[Return to top\]](#)

Postal and Shipping Sector

13. *April 13, WCAU 10 Philadelphia* – (Delaware) **Fire marshal investigates exploding mailbox.** The Delaware State Fire Marshal's office is searching for the person or people responsible for allegedly using explosives to damage a mailbox outside a home. It happened April 12 in Back Creek near Middletown. A homeowner discovered the mailbox damaged from an explosion, according to investigators.

Source: <http://www.nbcphiladelphia.com/news/local/Fire-Marshal-Investigates-Exploding-Mailbox--147310995.html>

14. *April 12, KPAX 8 Missoula* – (Montana) **Mail box blown up, Missoula PD investigating.** Police in Missoula, Montana, say they are looking into an April 11 incident where two juvenile boys blew up a mail box. The incident is still under investigation because police are trying to determine what they used as an explosive device.
Source: <http://www.kpax.com/news/mail-box-blown-up-missoula-pd-investigating/>

[\[Return to top\]](#)

Agriculture and Food Sector

15. *April 13, USA Today* – (National) **Drought expands throughout USA.** The United States has not been as dry as it is now in almost 5 years, USA Today reported April 12. Still reeling from devastating drought in 2011 that led to at least \$10 billion in agricultural losses across Texas and the South, the nation is enduring another unusually parched year. A mostly dry, mild winter put nearly 61 percent of the lower 48 states in “abnormally dry” or drought conditions, according to the U.S. Drought Monitor, a weekly federal tracking of drought. That is the highest percentage of dry or drought conditions since September 2007. Only two states — Ohio and Alaska — are entirely free of abnormally dry or drought conditions. The drought is expanding into some areas where dryness is rare. According to the U.S. Geological Survey, stream levels are at near-record or record lows in much of New England. The Drought Monitor lists all of Vermont as “abnormally dry,” just 6 months after the state’s wettest August on record that stemmed mainly from disastrous flooding by the remnants of Hurricane Irene. The rest of the East is also very dry. More than 63 percent of Georgia is in the worst two levels of drought, the highest percentage of any state. Wildfires and brush fires have been common along the East Coast from New England to Florida in recent weeks. Trouble also looms for water-dependent California. The state department of water resources announced the week of April 2 that water content in California’s mountain snowpack is 45 percent below normal.
Source: <http://www.usatoday.com/weather/drought/story/2012-04-11/mild-winter-expands-usa-drought/54225018/1>
16. *April 13, WGHP 8 High Point; Associated Press* – (North Carolina) **Cold damages apples in western North Carolina.** Agriculture officials said the cold snap the week of April 9 damaged the apple crop in the western North Carolina mountains. The Henderson County county extension agent said he saw damage April 12, and more cold weather occurred early April 13. A freeze watch was in effect in western North Carolina for early April 13. Temperatures hovered around the freezing mark or just below freezing. The extension agent said it will take a few days to determine the amount of damage. He said temperatures below 29 degrees can damage crops. Apple trees had bloomed about 2 weeks early because of the mild winter. A Henderson County grower said frost ravaged his 10 acres of peach trees, and his apple crop also was affected.
Source: <http://myfox8.com/2012/04/13/cold-damages-apples-in-western-north-carolina/>

17. *April 13, KERO 23 Bakersfield* – (California) **New cell phone app helps stop citrus diseases.** A new cell phone application called, Save Our Citrus, was created by the U.S Department of Agriculture to provide information about the Asian Citrus Psyllid and the disease it can carry, KERO 23 Bakersfield reported April 13. Users can identify and report possible citrus pests and diseases with a simple touch of their screen using the free app. “You don’t need to know what the bug looks like. This app has descriptions and photos of what happens to the actual tree so you can actually report. You can get the GPS location and send it right to the authorities,” said the executive director of the Kern County Farm Beureau. The Asian Citrus Psyllid carries a disease that causes the fruit to become dry and bitter and the tree dies.
Source: <http://www.turnto23.com/news/30885808/detail.html>
18. *April 12, Associated Press* – (Kansas) **Kansas grain elevator cited for serious violations.** The federal government cited a Missouri grain company April 12 for willful safety violations and proposed a hefty fine for an explosion that killed six workers in October 2011 at a northeast Kansas grain elevator. The U.S. Labor Secretary said in a news release the deaths at the Bartlett Grain Co. elevator in Atchison “could have been prevented” if the operators had addressed hazards known in the industry. The Occupational Safety and Health Administration (OSHA) is seeking \$406,000 in penalties in addition to the citations alleging five willful and eight serious safety violations. Kansas investigators previously found the October 29, 2011, grain dust explosion was accidental. Two other workers were injured in the blast in Atchison, about 50 miles northwest of Kansas City. Among the willful violations, the OSHA says the firm allowed grain dust, which is nine times as explosive as coal dust, to accumulate and used compressed air to remove dust without first shutting down ignition sources. The OSHA defines a willful violation as one committed with intentional knowing or voluntary disregard for the law’s requirements or with plain indifference to worker safety and health. The serious violations include claims that there was a lack of preventative maintenance, and that the housekeeping program was deficient because it did not prevent grain dust accumulations. The president of Bartlett Grain, said in a written statement that the company plans to prove wrong “OSHA’s unfortunate citations and characterization.”
Source: <http://www.deseretnews.com/article/765568147/Kansas-grain-elevator-cited-for-serious-violations.html>
19. *April 12, WIFR 23 Rockford* – (Illinois) **Illinois Department of Agriculture to spray 3,500 acres in Winnebago Co. for gypsy moths.** The Illinois Department of Agriculture will spray 3,500 acres for gypsy moths, WIFR 23 Rockford reported April 12. The areas that will be treated are just north of Interstate 39 in Rockford and four smaller areas in rural Winnebago County near Shirland. The treatment is being applied early this year in late April and May because of the high temperatures. A pheromone will be used in Rockford instead of pesticides.
Source:
http://www.wifr.com/news/headlines/llinois_Department_of_Agriculture_to_Spray_147269535.html?ref=535

20. *April 12, Belleville News-Democrat* – (Illinois) **Millstadt grain elevator closes, surrenders license.** A Millstadt, Illinois grain elevator closed and surrendered its license April 12 to the Illinois Department of Agriculture. A department spokesman said the Handy Feed & Grain Co. was closed April 2 after the department discovered the grain elevator had insufficient assets to meet provisions required under the Illinois Grain Code. The business is a member of the Illinois Grain Insurance Fund, which means all grain deposits at the elevator are protected.
Source: <http://www.bnd.com/2012/04/12/2138213/millstadt-grain-elevator-closes.html>
21. *April 11, US Food Safety* – (National) **Carta Blanca, Dos Equis Ambar, and Indio beer recalls.** Heineken USA of White Plains, New York, announced a recall of several products and packages in specific states due to a defect in the 12-ounce brown bottles used for certain batches of Carta Blanca and Dos Equis Ambar, which are available in 6-packs and 12-packs as well as Beers of Mexico and Best of Mexico pack varieties, US Food Safety reported April 11. Indio 12-ounce bottles, which are only featured in the Best of Mexico pack (available only in Texas), are also affected. The affected bottles were produced by a third party supplier and the defect was detected through routine quality inspections. Due to this defect, there is the potential for small grains or particles of glass to separate from the inside lip of the bottle and fall into the liquid. The pieces may vary in size and some may not be easily visible. The products are being recalled in 43 states.
Source: <http://www.usfoodsafety.com/zr120070.aspx>

For another story, see item [22](#)

[\[Return to top\]](#)

Water Sector

22. *April 13, Roanoke Times* – (Virginia) **Chlorine kills fish near Christiansburg treatment plant.** A procedure at Christiansburg, Virginia's wastewater treatment plant led to 12 pounds of chlorine killing several hundred fish, a spokesman with the Virginia Department of Environmental Quality (DEQ) said April 12. The spill occurred April 10 during a procedure to identify a leak, officials said. Chlorine was used to pinpoint the leak, which led to it spilling into Crab Creek. Officials said the problem was addressed and DEQ was awaiting a final count from biologists on the number of fish killed. It is not considered a major incident at this point, but reports indicate that about half a mile of stream was affected.
Source: <http://www.roanoke.com/news/roanoke/wb/307422>
23. *April 12, Battle Creek Enquirer* – (Michigan) **Albion oil spill into Kalamazoo River contained.** Barrels of old petroleum products were apparently dumped into a storm drain at the former Union Steel plant and eventually flowed into the Kalamazoo River, the Battle Creek Enquirer reported April 13. The interim city manager and police chief said a preliminary investigation showed people dismantling the plant for scrap metal may have dumped liquids into the drain before hauling away metal barrels. An on-scene coordinator for the U.S. Environmental Protection Agency (EPA) said the liquids

are likely waste oil and transmission fluid left behind in the building. He said as many as 30 barrels may have been removed but he can not estimate the amount of liquid dumped into the drain. Workers found oil on the floor leading to a trench and eventually to the storm drain. About a dozen more barrels of the oil are being cleared out of the building by a contracting company. Officials do not expect any lasting environmental damage and crews placed containment booms in the river. The first priority of the EPA is cleaning the spill and then determining who should pay the expenses.

Source:

<http://www.battlecreekenquirer.com/article/20120412/NEWS01/304120010/Albion-oil-spill-into-Kalamazoo-River-contained?odyssey=tab|topnews|text|Frontpage>

24. *April 12, Associated Press* – (Washington) **Broken Everett sewer pipe leaks into creek.** A broken sewer pipe in south Everett, Washington, spilled what a city spokeswoman estimates as “hundreds of thousands of gallons” of sewage April 12 into a creek that eventually flows into Lake Washington. She said crews were able to divert the sewage flow into pump trucks and put that material back into the sewage system at a different point. Crews were repairing the 20-inch pipe and officials stated the drinking water supply was safe. Residents were, however, cautioned to avoid contact with water in North Creek. The spokeswoman said sewage got into the crawl space of one home but no other properties were affected. The state ecology department and other agencies were notified of the spill.

Source:

http://seattletimes.nwsourc.com/html/localnews/2017969893_apwabrokeneverettsewepipe1stldwritethru.html

25. *April 12, Associated Press* – (California) **Software flaw, mistake led to raw sewage spill.** A software malfunction and operator error are to blame for a 2-million-gallon raw sewage leak into the Tijuana River in California, April 4, according to the owner of the South Bay International Wastewater Treatment Plant. Failures at the San Ysidro plant were first revealed publicly by environmental groups, the Surfrider Foundation and Wildcoast, according to U-T San Diego. The plant’s operator, Veolia Water North America, filed a spill notice with the state in about 2.5 hours. Reports were made with local agencies, too. Environmental groups criticized officials for not doing more to alert residents. The plant was built to process about 25 million gallons of sewage a day from Tijuana, Mexico, and then discharge it into the ocean. The intention is to reduce contamination from wastewater from Mexico on southern California waterways and beaches. The county water quality chief said the system failure had little impact on the heavily polluted river.

Source: http://www.mercurynews.com/breaking-news/ci_20385563/software-flaw-mistake-led-raw-sewage-spill

For more stories, see items [4](#) and [15](#)

[\[Return to top\]](#)

Public Health and Healthcare Sector

26. *April 13, Fort Lauderdale Sun Sentinel* – (Florida) **Patient ID information stolen at Memorial hospitals.** Patients of Memorial hospitals in Broward County, Florida, had their identities stolen by employees who wanted to use the information to make money filing phony tax returns, Memorial officials said April 12. Two employees were fired and are under criminal investigation by federal agents for improperly gaining access to the patients' data, said a spokeswoman for tax-assisted Memorial Healthcare System, parent of five Memorial hospitals. Memorial sent letters to about 9,500 patients whose identities may have been exposed by the two employees. The spokeswoman could not say how many of the 9,500 identities were stolen or whether any of them were misused to file false tax returns.
Source: <http://www.sun-sentinel.com/business/fl-memorial-hospital-id-theft-20120412,0,1899503.story>
27. *April 12, Miami Herald* – (Florida) **Miami doctor convicted in pill-mill racket that revolved around County Hall pharmacy.** A federal jury found a Miami physician guilty of conspiracies to defraud the government healthcare program and to peddle oxycodone and other pain-killers, the Miami Herald reported April 12. The doctor's role: signing about 6,700 prescriptions at a network of local clinics. The scheme featured the physician collaborating with clinic and pharmacy owners to distribute oxycodone and oxymorphone to purported patients who received kickbacks. Since 2007, Medicare reimbursed the pharmacies \$15 million, and the illicit drugs were resold on the street for \$40 million, according to federal prosecutors.
Source: <http://www.miamiherald.com/2012/04/12/2745329/miami-doctor-convicted-in-pill.html>
28. *April 12, Associated Press* – (Ohio) **Review says Ohio hospital has security lapses.** The Associated Press reported April 12 that the government plans to end federal Medicare funding to Adena Medical Center in Chillicothe, Ohio, after inspectors said security lapses were serious enough to “pose immediate jeopardy to patient health and safety.” WBNS 10 Columbus reports an Ohio Department of Health review says that in February, a discharged patient took a nurse's badge and stole medications from a secure unit. Officials said they found two areas with unsecured drugs and syringes in March. However, a spokeswoman told media outlets April 11 that the hospital expects to avert the cut-off, set for April 27, by complying with security rules before then. She said policies that started in March include requiring visitor badges and updates to check-in procedures.
Source:
http://www.wtap.com/news/headlines/Review_Says_Ohio_Hospital_Has_Security_Lapses_147220465.html

[\[Return to top\]](#)

Government Facilities Sector

29. *April 13, Associated Press* – (Alaska) **2 dead in shooting at Alaska station; FBI on scene.** Two U.S. Coast Guard members were found shot to death at work in Kodiak Island, Alaska, in what officials said appeared to be a double homicide. Another Coast Guard member found the victims April 12 at their work areas inside the communications station, a spokeswoman said. She said officials believed a third person was involved, but no suspect was in custody or identified as of April 12. A captain said he was not aware of any threats or anything else that might have indicated problems at the station. After the shooting, security was increased at the base, about 8 miles from the island’s largest city of Kodiak. Added security also was put in place at an adjacent school. A petty officer said the station has “secure front doors,” and requires staff and visitors to show identification. The spokeswoman said visitors and those not actually working at the station are usually provided escorts.
Source: <http://www.foxnews.com/us/2012/04/13/2-dead-in-shooting-at-alaska-station-fbi-on-scene/>
30. *April 13, Associated Press* – (Colorado) **TCA president resigns after suspicious device incident.** The Classical Academy (TCA) Board of Directors accepted the resignation of their president and placed a high school principal on administrative leave April 9 after an incident at TCA North Campus in Colorado Springs, Colorado, where two camping propane tanks, marginally functioning flares, rubbing alcohol, a fuel cell for a model rocket, and some boxer shorts were found in two separate suspicious packages. The board of directors was informed of a third device identified prior to the incident, which took place the week of April 2 and prior to spring break (March 26-30), which may have been related to the other two. The device was determined to be a jar of rubbing alcohol and various smoking fireworks by the Colorado Springs Police Department. The device was determined to be incendiary like the other two, and also did not have an ignition source.
Source: <http://www.krdo.com/news/30868144/detail.html>
31. *April 12, Government Computer News* – (National) **Oak Ridge team using advanced machine learning to counter cyber threats.** Oak Ridge National Lab in Oak Ridge, Tennessee, is developing many cybersecurity tools that use advanced machine learning to counter cyber threats, Government Computer News reported April 12. One tool under development looks for data being sent from inside an enterprise by insiders, leveraging data from each host on the network to identify bad behavior. The lab was the victim of one of the most notable breaches of 2011, after which it was offline for more than a week. A successful phishing attack infected its network with what a spokesperson called a “very sophisticated” piece of malware apparently designed to steal information from the lab’s network. E-mail and Internet access at the lab were shut down until the infection could be identified and removed.
Source: <http://gcn.com/articles/2012/05/07/feature-1-oak-ridge-big-security-sidebar.aspx>

For another story, see item [7](#)

[\[Return to top\]](#)

Emergency Services Sector

32. *April 13, New York Daily News* – (New York) **Cops warned of ‘Drano bomb’ threat.** The New York City Police Department (NYPD) in the Rockaways was targeted for an attack with “Drano bombs,” the New York Daily News learned. The NYPD issued a citywide alert April 10 warning officers about “Drano bombs,” also known as “bottle bombs,” that “are exploded by readily mixing available household products in plastic containers.” Police sources said that while the alert went to every precinct, the greatest concern is in the Rockaways. The sources said police recently learned from informants that gang members and other troublemakers talked about throwing bombs at police officers or placing them near patrol cars. A second source said police are trying to determine if the plot is tied to any recent police activity — such as a major arrest or initiative — or if someone heard about it on the Internet and spread the word.

Source: <http://www.nydailynews.com/new-york/cops-warned-drano-bomb-threat-article-1.1061036>

33. *April 12, Charleston Daily Mail* – (West Virginia) **Police say patient stabbed paramedic in head, stole ambulance.** Police said a Nicholas County, West Virginia man stabbed a paramedic and stole his ambulance April 10. A police deputy was dispatched to help a paramedic with a combative patient when the patient grabbed a pair of scissors and stabbed the paramedic in the head, according to a criminal complaint filed in Nicholas Magistrate Court. He then took off in the ambulance, owned by Quinwood Ambulance. The paramedic suffered serious injuries and was taken to a local hospital. The patient then crashed the ambulance into a tree, destroying nearly 100-feet of guardrail in the process, the complaint said.

Source: <http://www.dailymail.com/policebrfs/201204120144>

[\[Return to top\]](#)

Information Technology Sector

34. *April 13, Computerworld* – (International) **Apple delivers Flashback malware hunter-killer.** Two days after Apple promised to decontaminate Macs infested with the Flashback malware, the company delivered. The newest Mac OS X Java update issued April 12 includes a tool that will “remove the most common variants of the Flashback malware,” Apple’s advisory read. April 10, Apple for the first time acknowledged the Flashback malware campaign that exploited a Java vulnerability to infect hundreds of thousands of Macs. At the same time, Apple pledged to craft a detect-and-delete tool that would scrub compromised machines of the attack code. The April 12 update also disables automatic execution of Java applets in the Java browser plug-in; the exploit used by Flashback to infect Macs was hidden inside a malicious Java applet hosted on compromised Web sites. One of the reasons Flashback was able to infect so many Macs was because the Java plug-in automatically ran the offered applet. Apple’s move is a step toward disabling Java, the advice most security experts suggest to users.

Source:

http://www.computerworld.com/s/article/9226175/Apple_delivers_Flashback_malware_hunter_killer

35. *April 13, The H* – (International) **Firefox gets click-to-play option for plugins.** A software engineer at Mozilla created an implementation of “click-to-play plugins” for Firefox. With this enabled, the browser will require that content from plugins like Flash and Java be clicked before the plugin loads and runs. The feature, which Mozilla also calls “opt-in activation for plugins” is already accessible in nightly builds of Firefox and the engineer is working on giving the browser the ability to remember click-to-play settings on a site-by-site basis. A security benefit of the click-to-play approach is that plugins only get loaded when the user actually clicks on the content in question. This limits the opportunities for “drive-by” malware attacks by malicious content that targets plug-in vulnerabilities in Flash and Java. The feature could help prevent the spread of malware such as the Flashback trojan, as Java would only be loaded if the user expects legitimate Java content on the page in question and clicks on it. However, malware creators can still use social engineering to encourage users to click anyway.
Source: <http://www.h-online.com/security/news/item/Firefox-gets-click-to-play-option-for-plugins-1520514.html>
36. *April 13, The Register* – (International) **New fake anti-virus shakes down frightened file-sharers.** Security researchers discovered a strain of fake anti-virus software that tries to intimidate supposed file-sharers into paying for worthless software. SFX Fake AV, first detected by antivirus scanner firm Malwarebytes, blends the features of scareware with those more associated with ransomware trojans. The malware stops any legitimate antivirus package from running on compromised PCs. This particular strain of malware also stops Process Explorer and prevents browsers from loading — tactics designed to force users to complete the “input credit card details” screen and pay money for the scamware. The app also falsely tells victims they are going to be sued for breaching anti-piracy legislation, claiming it detected torrent links on PCs. It offers to get around this problem by activating an “anonymous data transfer protocol” for torrent links, another inducement aimed at persuading users into paying for the worthless security app. This latter feature differentiates the malware from strains of scareware seen in the past, which demand money after supposedly detecting “offensive materials” on PCs. The malware also performs a fake scan that classifies Windows Registry Editor as a pornography tool. The vice president of research at Malwarebytes said: “SFX Fake AV is morphing at a relatively fast rate, so it is something that signature-based vendors will have to watch out for as there will be an increasing number of variants in the wild. Also, the use of Dropbox as a delivery mechanism is something that the industry is going to have to take into account and protect against, as it is an emerging trend.”
Source: http://www.theregister.co.uk/2012/04/13/scareware_ransomware_hybrid/
37. *April 12, The H* – (International) **Facebook SDK hole leaves accounts vulnerable.** A developer discovered a vulnerability in the Facebook software development kit (SDK) for Android that grants specially crafted Android applications unauthorized access to the smartphone owner’s Facebook account. Apps such as Foursquare use the SDK as a way to read users’ Facebook profiles or post photos to their walls; usually, this requires additional permissions to be requested from the user. Once those permissions are

granted, the app receives an access token from the Facebook server that, until revoked, enables it to perform the requested actions. The developer found that, with the required permissions in place, the Facebook SDK writes a URL that contains the token to a log file on the smartphone — and this log file is accessible by any app given permission to “Read Sensitive Log Data” during installation. As many Android users automatically confirm permission requests when installing apps, it should not be difficult for attackers to obtain the required access. Using the stolen access token, a specially crafted app could then obtain any permissions granted to the token’s legitimate app.

Source: <http://www.h-online.com/security/news/item/Facebook-SDK-hole-leaves-accounts-vulnerable-1519859.html>

38. *April 12, IDG News Service* – (International) **Oracle to issue 88 security patches on Tuesday.** Oracle plans to release 88 patches April 17, covering vulnerabilities affecting a wide array of products, according to a pre-release announcement posted to its Web site April 12. The upcoming patch batch includes six fixes for Oracle’s database, three of which can be exploited remotely without a username and password. The highest Common Vulnerability Scoring System (CVSS) base score for the database bugs is 9 on the system’s 10-point scale. Another 11 patches cover Oracle Fusion Middleware, with 9 being remotely exploitable without authentication. Within this group, the highest CVSS base score is 10 for Oracle JRockit. Other affected products include BI Publisher and JDeveloper. The patch release also includes 6 bug-fixes for Oracle Enterprise Manager Grid Control; 4 for the E-Business Suite enterprise resource planning application; 5 for Oracle’s Supply Chain Suite; 15 for various PeopleSoft Enterprise applications; 17 for Oracle Financial Services software; 2 for Oracle Industry Applications; and 1 for Oracle Primavera. Another 15 cover Oracle Sun products, including the GlassFish application server and the Solaris OS. Oracle is also set to ship six patches for the MySQL database.

Source:

http://www.computerworld.com/s/article/9226169/Oracle_to_issue_88_security_patches_on_Tuesday

39. *April 12, Threatpost* – (International) **Tough love triumphs: SCADA vendor Koyo fixes Basecamp bugs.** Industrial control system vendor Koyo moved to fix vulnerabilities in its ECOM brand programmable logic controllers (PLCs) after researchers, in January, revealed the devices were vulnerable to brute force password guessing attacks. The U.S. Industrial Control Systems Cyber Emergency Response Team issued an advisory April 11 that said the company issued a patch for affected ECOM modules that disables a vulnerable Web server and adds a “timeout” feature to prevent brute force attacks on the device password. Koyo was one of a number of supervisory control and data acquisition and industrial control systems (ICS) vendors whose products were targeted by researchers as part of Project Basecamp, a volunteer effort to expose rampant product insecurity in the ICS sector.

Source: http://threatpost.com/en_us/blogs/tough-love-triumphs-scada-vendor-koyo-fixes-basecamp-bugs-041212

For more stories, see items [31](#), [40](#), [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 13, IDG News Service* – (International) **ICANN postpones cutoff date for new gTLD applications after glitch.** The Internet Corporation for Assigned Names and Numbers (ICANN) has postponed the last date for applications for new generic top-level domains (gTLDs) on its application system to April 20, after it detected a technical issue with the software. The organization said in a statement that it had to take the TLD application system (TAS) offline temporarily after it learned of a possible glitch in the software that has allowed “a limited number of users to view some other users’ file names and user names in certain scenarios. Out of an abundance of caution, we took the system offline to protect applicant data. We are examining how this issue occurred and considering appropriate steps forward,” ICANN’s chief operating officer said in a statement April 12. TAS will be shut down until April 17, unless otherwise notified before that time, the ICANN said.
Source: <http://www.networkworld.com/news/2012/041312-icann-postpones-cutoff-date-for-258247.html?hpg1=bn>

For another story, see item [37](#)

[\[Return to top\]](#)

Commercial Facilities Sector

41. *April 13, CNN* – (Ohio) **Three dead in Ohio restaurant shooting.** An apparent domestic dispute left three people dead at a Cracker Barrel Old Country Store and Restaurant in Brooklyn, Ohio, April 12, according to police. The shootings took place after police received a 9-1-1 call from a woman at the restaurant. The woman told police that her husband was in a car circling the eatery. When officers arrived, they heard gunshots and encountered a man leaving the restaurant with a gun. When the gunman failed to surrender to authorities, they fatally shot him. In addition to the gunman, a woman and a girl were dead at the scene. Another girl was wounded and transported to a local hospital for treatment.
Source: http://www.cnn.com/2012/04/13/justice/ohio-shooting/index.html?hpt=us_c2
42. *April 13, San Antonio Express-News* – (Texas) **Vapor leak at gym sends three to hospital.** Three children were taken to a hospital, April 12, after being exposed to a vapor at a fitness center in San Antonio that caused ear, nose and throat irritation. Three children and three teenagers who had been in the pool area complained of eye, nose,

and throat irritation. The building was evacuated for about an hour and firefighters discovered a container of chlorine and a container of hydrochloric acid that could have caused the symptoms. The teens were treated at the scene and the children were taken to a hospital as a precaution.

Source: http://www.mysanantonio.com/news/local_news/article/Vapor-leak-at-gym-sends-three-to-hospital-3478904.php

43. *April 13, Canton Repository* – (Ohio) **Fire guts Canton Township business, apartments.** Firefighters from five departments battled a fire that destroyed a skill games business and two apartments in Canton Township, Ohio, April 12. The fire at the Uncle Sam’s Skill Games also shut down several blocks of Lincoln Street for nearly 8 hours. The Canton Township fire chief said firefighters called to battle a basement fire arrived to find flames consuming the business, an apartment above it, and another attached to the side of it. They found an open gas line in the basement with no way to shut it off, causing the firefighters to move to a defensive posture until the gas was shut off. Firefighters believed the fire started in the basement. The cause remained under investigation, the chief said.

Source: <http://www.cantonrep.com/news/x1830127270/Fire-closes-Lincoln-Way-East-at-Trump-Road>

44. *April 13, Albany Times Union* – (New York) **Desmond reports serious credit card security breach.** The Desmond hotel in Colonie, New York, said a “serious data security breach” compromised guests’ credit card information spanning 10 months between May 2011 and March, the Albany Times-Union reported April 13. In a letter to customers posted on its Web site, the hotel and conference center said an “outside party” accessed the hotel’s computer system — including guests’ full names, credit and debit card numbers, card expiration dates, “service codes,” and any other “discretionary data” contained in the cards’ magnetic strips. The hotel said a cyber-security firm recommended to it by the U.S. Secret Service found no evidence that customers’ debit card pin numbers were accessed. “This is a serious incident,” the letter read, urging customers who may have been affected to contact the three main credit reporting agencies to check for fraud.

Source: <http://www.timesunion.com/local/article/Desmond-reports-serious-credit-card-security-3479978.php>

45. *April 13, CNN* – (Indiana) **Reports: Indiana State Fair stage where seven died was inadequate.** Scaffolding that collapsed during a storm and killed seven people during the Indiana State Fair in 2011 was not up to standard, and the fair’s commission did not have adequate emergency planning in place, according to two investigative reports presented April 12. “Calculations and in-situ physical testing determined the Jersey barrier ballast (support) system had grossly inadequate capacity to resist both the minimum code-specified wind speed (68 miles per hour) and the actual wind speed that was present at the time of the failure (approximately 59 miles per hour),” according to a report by Thornton Tomasetti Inc., an engineering firm. The National Weather Service had estimated winds of 60 to 70 mph were raking the area when the incident occurred in August 2011. A massive gust of wind brought down the stage, killing five people and injuring dozens. Two others later died as a result of the collapse.

Source: http://www.cnn.com/2012/04/12/us/indiana-state-fair-reports/index.html?hpt=us_c2

For more stories, see items [25](#), [46](#), and [48](#)

[\[Return to top\]](#)

National Monuments and Icons Sector

46. *April 13, Roanoke Times* – (Virginia) **Wildfires burning 20,000 acres in national forest areas.** Crews fighting major southwest Virginia wildfires were battling blazes that, collectively, reached historic proportions — and led officials to close some surrounding areas to the public April 13. “Right now, when you look at the entire George Washington National Forest, we have 20,000 acres on fire,” said a head ranger for the Warm Springs and James River district of the George Washington and Jefferson National Forests. The three largest fires near the Roanoke area — at Alleghany Tunnels, Rich Hole, and Barbours Creek — all grew significantly between April 11 and 12. Of the three major fires in the area, the only one threatening buildings was the fire in the Barbours Creek Wilderness. Four residences northeast of the fire had been secured, and the Potts Mountain Jeep Trail and Pines Campground were closed. Source: <http://m.roanoke.com/mapp/story.aspx?arcID=307420>

For another story, see item [15](#)

[\[Return to top\]](#)

Dams Sector

47. *April 13, Bergen County Record* – (New Jersey) **Report that absolves Pompton Lakes Dam floodgates stirs up a storm.** A study commissioned by the New Jersey Department of Environmental Protection (DEP) released April 12 says the much-criticized Pompton Lake Dam in Passaic County, New Jersey, is not responsible for massive flooding that occurred downstream since 2010. The nearly 600-page report found the floodgates worked correctly during Tropical Storm Irene in August 2011 and during flooding in March 2010 and March 2011 and instead blames a significant increase in rainstorms and their intensity for the damage. The study noted that northern New Jersey has had 50 to 65 more inches of rain in the past 72 months than normal, and that the average peak stream flow along the Ramapo River near Mahwah over the past decade was 55 percent higher than the average over the prior 60 years. Rainfall amounts from Irene in August 2011 amounted to a 500-year event in the river system’s upper watershed and a 100-year event in the lower watershed, the report said. The DEP has provided \$350,000 in grants to Wayne, Pequannock, Riverdale, and Pompton Lakes for a pilot project to remove snags, debris, and shoals in the river system that exacerbate flooding. In addition, the DEP will begin working with the U.S. Army Corps of Engineers on a study in June to determine what structural improvements can be made to help reduce flooding long term, including flood walls, flood storage areas, and channel dredging.

Source:

http://www.northjersey.com/news/Pompton_Lakes_Dam_floodgates_not_responsible_for_extensive_flooding_report_says.html?page=all

48. *April 13, Associated Press* – (California) **Push launched to upgrade levees, keep Silicon Valley above water.** Business leaders and a U.S. Senator from California launched a \$1 billion, 10-year fundraising goal April 12 aimed at preventing some of Silicon Valley's leading technology companies from going underwater — literally. The money is being sought to build a new earthquake- and storm-proof levee system along the southern part of San Francisco Bay, where the corporate campuses of Facebook, Google, and other high-tech ventures abut land drained a century ago for commercial salt-making. Planners predict those sites and thousands of South Bay homes are at risk of catastrophic flooding over the next half-century due to a climate change-fueled sea level rise. Currently, the bay's tidal waters are contained by low-lying levees constructed more than 100 years ago to create salt ponds, and they would be inadequate to the task of protecting prime real estate even if they were not deteriorating, the president of the Gordon and Betty Moore Foundation said.

Source: http://www.timesheraldonline.com/ci_20388064/push-launched-upgrade-levees-keep-silicon-valley-above

[[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

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.