



## Daily Open Source Infrastructure Report 16 July 2012

### Top Stories

- Two Dallas men were indicted July 12 in connection with a \$485 million investment fraud scheme that swindled money from more than 7,700 investors throughout the country. – *Federal Bureau of Investigation* (See item [14](#))
- An international commuter tunnel connecting Detroit to Windsor, Ontario, was closed for nearly 4 hours July 12 after a bomb threat was phoned in on the Canadian side. – *Associated Press; CBS News* (See item [17](#))
- A severe drought spreading across the Midwest has resulted in some of the worst conditions in decades, leaving more than 1,000 counties in 26 States designated as natural disaster areas, authorities said. – *CNN* (See item [25](#))
- Thousands of patients of two Denver-area practices were advised to get tested July 12 after a licensed dentist and practicing oral surgeon may have exposed them to HIV, hepatitis B, and/or hepatitis C over a period of 11 years. – *KUSA 9 Denver* (See item [30](#))

---

### 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

1. *July 13, New Mexico Business Weekly* – (New Mexico) **Western Refining to pay \$444,000 for emissions violations.** The New Mexico Environment Department (NMED) has reached a settlement with Western Refining over emissions violations for \$444,000, the New Mexico Business Weekly reported July 13. The violations allegedly took place between July 1, 2009, and March 15, 2012, at the company’s Ciniza refinery near Gallup. Under the agreement, Western Refining has agreed to pay the monetary fine for “excess emissions of sulfur dioxide, nitrogen oxides and other pollutants,” according to a news release. In addition to paying the \$444,000 fine, an agreement obligates Western Refining to undertake various upgrades and infrastructure improvements at the Ciniza refinery over the next several years. These improvements are designed to lower the emissions of regulated pollutants. Western Refining is an independent oil refiner and marketer with retail, wholesale and refining offices in New Mexico.  
Source: <http://www.bizjournals.com/albuquerque/blog/morning-edition/2012/07/western-refining-to-pay-444000-for.html>
2. *July 13, WOWK 13 Huntington* – (Kentucky) **MSHA proposes \$594,000 in fines for KY coal company.** The U.S. Mine Safety and Health Administration (MSHA) proposed \$594,100 in fines to a Kentucky coal company July 12 for violations related to a 2011 mine fatality. The fines against Manalapan Mining Co. Inc.’s P-1 Mine in Harlan County, Kentucky, are for four violations. The proposed penalties were assessed after an investigation into the June 2011 death of a miner who was fatally injured when a large section of rock fell from the underground coal mine’s wall, or rib, and knocked him into a dolly.  
Source: <http://www.wowktv.com/story/19015047/msha-proposes-54>
3. *July 12, Associated Press* – (Kentucky) **Regulators fine utility \$24,000 for violations.** A Louisville, Kentucky utility has been fined \$24,000 for alleged violations that sent dust and odors into a neighborhood near a generating station. The Louisville Courier-Journal reported the Louisville Metro Air Pollution Control Board notices of violation, which date back to February, were made public July 11. The notices allege ash and sludge-handling violations. A Louisville Gas & Electric spokeswoman told the newspaper the company was in the process of reviewing the notices. An air district spokesman said district officials now want the company to come up with a plant-wide suppression plan for dust.  
Source: <http://www.kentucky.com/2012/07/12/2256228/regulators-fine-utility-24000.html>
4. *July 12, Rochester Business Journal* – (New York) **RG&E failed to protect customer info.** Rochester Gas and Electric Corp. (RG&E) and New York State Electric & Gas Corp. (NYSEG) failed to adequately protect confidential customer data from unauthorized access by outside parties, the State Public Service Commission (PSC) said July 12. The PSC investigation followed a January advisory from NYSEG that unauthorized parties obtained access to confidential information of its and RG&E customers. The data included Social Security numbers, dates of birth and, in some

cases, financial institution account information. There is no evidence any confidential information was misused, the PSC report stated. RG&E and NYSEG took reasonable actions to inform customers of the potential impacts of the breach, the investigation found, but several deficiencies in their systems and practices contributed to the breach. The companies have taken sufficient steps to prevent a recurrence, and are planning to revamp their information systems and data protection security, PSC officials said.

Source: <http://www.rbj.net/article.asp?aID=191850>

5. *July 10, Greentech Media* – (National) **Smart grid’s big data opportunities still untapped.** North American utilities may be collecting unprecedented amounts of data from millions of new smart meters — 18,000 percent more data, to be exact. That is one finding from a new survey from Oracle released July 10, covering the “big data” challenges and opportunities in the smart grid. The survey of 151 North American utility executives revealed a disconnect between data collection and putting that data to use. For instance, while 78 percent of respondents said their utilities were collecting outage detection data from smart meters, only 59 percent were actually using it for business processes and decision-making as of April 2012, when the survey was conducted. Similar gaps were revealed in voltage data (73 percent collecting it and 57 percent using it), tamper detection data (63 percent collecting it and 47 percent using it), and diagnostic data (56 percent collecting it and only 33 percent using it).

Source: <http://www.greentechmedia.com/articles/read/smart-grids-big-data-opportunities-still-untapped/>

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

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

## **Chemical Industry Sector**

See items [29](#), [32](#), [36](#), [37](#),

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

## **Nuclear Reactors, Materials and Waste Sector**

6. *July 13, Global Security Newswire* – (International) **Another infiltration reported at South African atomic site.** South Africa’s Pelindaba nuclear facility in April sustained an unspecified violation of its protective measures, marking the third such case at the site in 7 years, the Johannesburg Times reported July 12. Plant operator South African Nuclear Energy May 7 informed the “relevant” official agency of the incident, which Business Day said happened April 28. South Africa’s former apartheid government decades ago conducted nuclear arms research and production at Pelindaba, which now is used to prepare medical isotopes. South African Nuclear Energy and the National Nuclear Regulation both refused to provide details on the recent infiltration or describe protections at the facility. Pelindaba is believed to hold hundreds of pounds of highly enriched uranium, according to the Washington-based Nuclear Threat Initiative.

Source: <http://www.nti.org/gsn/article/new-infiltration-reported-south-african-atomic-plant/>

7. *July 12, Syracuse Post-Standard* – (New York) **Nine Mile Point 2 plant reactor shut down.** The Nine Mile Point nuclear power plant in Scriba, New York, shut down its Unit 2 reactor July 12 due to a decrease in condenser vacuum levels. The decrease was the result of a failure of a steam regulator. A Nuclear Regulatory Commission (NRC) official called the shutdown “uncomplicated.” The NRC’s Senior Resident Inspector assigned to Nine Mile Point responded to the plant’s control room and did not identify any concerns with operator response or equipment performance.

Source:

[http://www.syracuse.com/news/index.ssf/2012/07/nine\\_mile\\_point\\_2\\_plant\\_reactio.html](http://www.syracuse.com/news/index.ssf/2012/07/nine_mile_point_2_plant_reactio.html)

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

## **Critical Manufacturing Sector**

8. *July 13, U.S. Department of Labor* – (Illinois) **U.S. Department of Labor’s OSHA cites Sandwich Castings and Machine in Illinois for 20 violations including lack of machine guarding.** The U.S. Department of Labor’s Occupational Safety and Health Administration July 13 cited aluminum castings producer Trio Foundry Inc., which operates as Sandwich Castings and Machine, with 20 health and safety violations, including one willful and one repeat violation at its Sandwich, Illinois facility. Proposed penalties total \$113,300. The willful safety violation was for failing to protect the operator of a belt sander from “caught-in” hazards and rotating parts. The repeat safety violation involved a lack of guarding on an abrasive grinder wheel. Nine serious safety violations and two other-than-serious violations were also cited.

Source:

[http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=22689](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22689)

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

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

## **Defense Industrial Base Sector**

9. *July 13, Military Times* – (National) **Flight control failure grounds C-27J planes.** The U.S. Air Force grounded its fleet of C-27J cargo planes after an aircraft experienced a mechanical failure in part of its flight controls during a training sortie July 3. Air Force officials at the plane’s program office in Ohio ordered the grounding following the incident, which it is calling a “flight control problem,” said a statement provided by an Air Force spokeswoman. The Air Force ordered an investigation, but called it a precautionary measure. “The program office is working with the C-27J prime contractor, L-3 Communications, and the aircraft manufacturer, Alenia Aermacchi, to resolve the matter as quickly as possible, and return the C-27J fleet to normal flight

operations,” the statement said. It is unclear how long the fleet will be grounded, but it is expected to be resolved within 1 to 2 weeks for specific aircraft shown to exhibit similar issues. Officials are examining parts of the flight-control surfaces, parts on the wings that control altitude. The Air National Guard is the only U.S. military operator of the aircraft.

Source: <http://www.militarytimes.com/news/2012/07/air-force-c-27j-planes-grounded-flight-control-failure-071312d/>

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

## **Banking and Finance Sector**

10. *July 13, Softpedia* – (International) **FBI arrests 3 more individuals accused of carding crimes.** As a continuation of an operation where authorities apprehended 24 individuals suspected of being involved in payment card information trafficking in June, the FBI announced the arrests of three more suspects, bringing the number of defendants to 27, Softpedia reported July 13. One known as HellsAngel was arrested July 11 in Mumbai, India. Another that went by the username Swat Runs Train, and another called xTGxKAKAROT, were taken into custody in Canada and Colorado, respectively. Swat Runs Train was suspected of selling complete credit card details, including names, addresses, Social Security numbers, birth dates, and bank account information. The one known as HellsAngel was also believed to have offered the same type of data. He also sold remote desktop protocol (RDP) access data that could be utilized to breach computers. xTGxKAKAROT possessed around 170,000 credential sets, comprised of usernames and passwords, which could be used to access online accounts. He also made money by selling electronic devices he obtained as a result of his carding activities.

Source: <http://news.softpedia.com/news/FBI-Arrests-3-More-Individuals-Accused-of-Carding-Crimes-281157.shtml>

11. *July 13, Softpedia* – (California; Washington) **Rapper ‘Guerilla Black’ arrested for buying and using stolen payment card details.** A rap artist known as Guerilla Black was detained at his home in Los Angeles on suspicion of purchasing and using at least 27,257 stolen credit card numbers obtained by hackers from 2 restaurants from the Seattle area, Softpedia reported July 13. The two hackers were previously arrested and indicted. While the total losses were not yet known, the amount may be large, especially since only 137 of the cards were used to make purchases worth \$150,000. The rapper was charged with accessing a protected computer without authorization to further fraud, access device fraud, bank fraud, aggravated identity theft, and conspiracy to commit access device fraud and to commit bank fraud. He was also accused of conspiracy to access protected computers to further fraud.

Source: <http://news.softpedia.com/news/Rapper-Guerilla-Black-Arrested-for-Buying-and-Using-Stolen-Payment-Card-Details-281192.shtml>

12. *July 12, WLS 7 Chicago* – (Illinois) **‘Wicker Park Bandit’ pleads guilty to bank robberies.** The man authorities call ‘The Wicker Park Bandit’ pleaded guilty to three bank robberies July 12 in Chicago. The man was arrested in February. At the time, the

FBI said he was a suspect in as many as 10 bank robberies in and around Chicago's Wicker Park neighborhood.

Source: <http://abclocal.go.com/wls/story?section=news/local&id=8734402>

13. *July 12, Bloomberg News* – (Virginia) **Bank of Commonwealth ex-CEO, officials charged with fraud.** The former chief executive officer (CEO) of Norfolk, Virginia's Bank of the Commonwealth was among six people indicted for an alleged fraud conspiracy involving a coverup of the bank's financial condition from 2008 to 2011, Bloomberg News reported July 12. The former CEO who ran the bank for more than 3 decades was charged in a 25-count indictment. Three other former bank executives and two borrowers were also charged. The executives concealed shortfalls by overdrawing demand-deposit accounts to make loan payments and extending new loans or additional principal on existing loans to cover payment deficiencies, the indictment charged. Prosecutors are seeking \$71 million in criminal forfeiture. From 2008 until it closed in 2011, the bank lost almost \$115 million. The bank's failure will cost the United States, through the Federal Deposit Insurance Corporation, more than \$260 million.  
Source: <http://www.businessweek.com/news/2012-07-12/bank-of-commonwealth-ex-ceo-officials-charged-with-fraud>
14. *July 12, Federal Bureau of Investigation* – (National) **Dallas men indicted in \$485M investment fraud scheme.** Two Dallas men were indicted July 12 in connection with a \$485 million investment fraud scheme that involved investors throughout the country. The two men were charged with one count of conspiracy to commit mail fraud, and 10 counts of mail fraud. According to the indictment, the men, on behalf of Provident Royalties LLC, conspired with others to defraud investors in an oil and gas scheme that involved more than \$485 million and 7,700 investors. Specifically, beginning in approximately September 2006, the two men and other individuals made materially false representations and failed to disclose material facts to their investors to induce them into providing payments to Provident. These included false representations that the funds invested would only be used for the project the funds were raised for, that one of Provident's founders had previously been charged with securities fraud violations by the State of Michigan, and that funds from later investors were used to pay earlier ones.  
Source: <http://www.loansafe.org/dallas-men-indicted-in-485m-investment-fraud-scheme>
15. *July 12, Associated Press* – (New Mexico) **Auditor says New Mexico Finance Authority issued fake audit for 2011.** The New Mexico Finance Authority (NMFA), which makes billions of dollars in loans for public projects, faked its annual audit that was sent to creditors and investors for 2011, the State auditor said July 12. The State Auditor said he discovered the fake audit after the NMFA failed to submit its annual review as required by law. He said a fraudulent audit report had been produced for investors and creditors, but the firm that supposedly created that document confirmed it was not their work. The CEO of the NMFA called the matter "deeply concerning" but insisted it would have no effect on NMFA's ability to meet its financial obligations. He blamed the authority's former controller, who left in June, and said the NMFA took steps to rectify the issues as quickly as possible. He said that the NMFA alerted ratings agencies, investors, public officials, and law enforcement authorities.

Source:

<http://www.therepublic.com/view/story/ff2882b265e14c1b8f18109fbd54f746/NM--Faked-Audit>

16. *July 12, IDG News Service* – (International) **Artema Hybrid point-of-sale devices can be hacked remotely, researchers say.** Artema Hybrid, a point-of-sale terminal manufactured by VeriFone Systems, is vulnerable to attacks that could allow cyber criminals to steal payment card data and PIN numbers or alter transactions, said security researchers from security research firm Security Research Labs (SRLabs). The software running on the device — commonly referred to as the firmware — contains buffer overflow vulnerabilities in the network stack — the set of libraries that handle network communications, the founder and chief scientist of SRLabs, said July 12. An attacker could exploit these vulnerabilities to execute arbitrary code on the device. Source: <http://www.csoonline.com/article/710833/artema-hybrid-point-of-sale-devices-can-be-hacked-remotely-researchers-say>

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

## Transportation Sector

17. *July 13, Associated Press; CBS News* – (Michigan; International) **Detroit-Windsor Tunnel reopens after bomb threat.** An international commuter tunnel connecting Detroit to Windsor, Ontario, was closed for nearly 4 hours July 12 after a bomb threat was phoned in on the Canadian side. No explosives were found, CBS News reported July 13. The Detroit Windsor Tunnel, a busy border crossing beneath the Detroit River, was shut down after a duty free shop employee on the tunnel's Canadian plaza reported receiving a call about a bomb threat. The tunnel was closed and traffic on both sides of the river was directed to the nearby Ambassador Bridge, which spans the river, the tunnel's executive vice president said. Homeland Security, U.S. Customs and Border Protection, Detroit police, and other agencies flooded the plaza and entrance on the tunnel's U.S. side. The bomb threat also resulted in heightened security along the Ambassador Bridge, west of downtown Detroit. The 82-year-old tunnel stretches about 1 mile across the Detroit River, which is one of North America's busiest trade crossings. Cars and buses make up most of the traffic. About 4.5 million cars crossed in 2011. After the call came in, officials at the tunnel followed protocol that is established between the tunnel operators and local emergency services officials in consultation with U.S. Customs and Border Protection, tunnel officials said. Source: [http://www.cbsnews.com/8301-505245\\_162-57471753/detroit-windsor-tunnel-reopens-after-bomb-threat/](http://www.cbsnews.com/8301-505245_162-57471753/detroit-windsor-tunnel-reopens-after-bomb-threat/)
18. *July 13, Associated Press* – (Ohio) **Service restored after Ohio train crash, explosion.** A railroad operator said it has cleared the Columbus, Ohio site of a train derailment and explosion and restored full rail service in the area, the Associated Press reported July 13. Part of a train derailed July 12 on Norfolk Southern Corp. tracks north of downtown, and three tank cars carrying ethanol exploded, causing a fire that burned for hours. Norfolk Southern said the cars have been cleared from the site, and the second of two affected main-line tracks reopened July 13. The National Transportation

Safety Board began an investigation into what caused the crash. A board member said the train was traveling below the recommended speed before the crash, and its operators noticed no problems with the track as they approached the curve where it happened.

Source: <http://www.daytondailynews.com/news/ohio-news/service-restored-after-ohio-train-crash-explosion-1404379.html>

19. *July 13, Associated Press* – (Maryland) **Hazmat crews called after Southwest flight attendant falls ill.** Airline and transportation officials said a flight attendant became ill on a Southwest Airlines flight, prompting HAZMAT crews at Baltimore-Washington International Thurgood Marshall Airport (BWI) to check the air on the craft, the Associated Press reported July 13. It happened on Southwest Flight 709, which left Norfolk, Virginia, July 12 to head to BWI and then Chicago. The plane carried 134 passengers and 5 crewmembers. It landed at scheduled at BWI and the sickened flight attendant was taken to a local hospital. Maryland State transportation officials said HAZMAT crews sampled the air on the plane, and blamed a cleaning solvent for the incident. A Southwest spokeswoman said passengers headed to Chicago on another plane.  
Source: <http://travel.usatoday.com/flights/story/2012-07-13/Hazmat-crews-called-after-Southwest-flight-attendant-falls-ill/56189860/1>
20. *July 12, ABC News* – (New York; International) **No Bomb on Delta plane turned around mid-flight over suspicious wires.** Authorities fearing terror in the sky turned around a flight to Madrid, Spain, shortly after it took off from New York when a federal air marshal spotted suspicious wires in a rear lavatory — but after searching the returned plane they found no suspicious devices, ABC News reported July 12. Port Authority Police, New York City’s bomb squad, and members of the FBI Joint Terrorist Task Force responded after the flight, Delta 126, returned to the ground at New York’s John F. Kennedy International Airport. Passengers were taken off the flight in a “controlled evacuation,” sources told ABC News. Authorities had been proceeding with caution and intended to interview the person who found the wires, who was on a team of armed federal air marshals aboard the flight.  
Source: <http://news.yahoo.com/no-bomb-delta-plane-turned-around-mid-flight-025847646--abc-news-topstories.html>
21. *July 12, Amarillo Globe-News* – (Texas) **Truck hauling potatoes careens off bridge.** Texas Department of Public Safety officials closed U.S. Highway 287 between Memphis and Childress July 12 after a tractor-trailer carrying a load of potatoes hit a guardrail on a highway bridge and plunged into the river east of Memphis, officials said. The tractor-trailer caught fire and was completely burned. Traffic on U.S. Highway 287 returned to normal 7 hours after the closure.  
Source: <http://amarillo.com/news/local-news/2012-07-12/txdot-traffic-diverted-between-memphis-and-childress-after-truck-fire>

For more stories, see items [23](#), [27](#), and [28](#)

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



## Postal and Shipping Sector

22. *July 13, KTVT 11 Dallas-Fort Worth* – (Texas) **Local mailbox target of thieves ‘phishing’ scam.** Residents in Fort Worth, Texas, notified the U.S. Postal Service (USPS) July 12 of what appeared to be a phishing scam set up at a neighborhood mailbox. The scam is an example of a crime that, according to the local postal inspector, has resulted in 30 arrests across the metroplex since October 2011. Someone coated the internals of a large, blue stand-alone neighborhood mailbox with an adhesive. A man who lives in a home nearby called the USPS after realizing mail would stick to the surface as it was dropped into the box. The local postal inspector said it is a crime that surfaces occasionally, with thieves looking for money or identity information. The most common tactic they said was to push something sticky into the box in an attempt to grab mail and pull it back out. The postal service has trained mail carriers to look for the adhesive and report it. The mailbox that had been tampered with had been cleaned by the evening.

Source: <http://dfw.cbslocal.com/2012/07/13/local-mailbox-target-of-thieves-phishing-scam/>

23. *July 13, Vallejo Times Herald* – (California) **Cough-inducing odor forces evacuation of Vallejo post office.** Vallejo, California firefighters closed off several blocks of the city July 12 after three people at a U.S. Post Office took ill from a mysterious smell. Emergency personnel responded when a clerk at the post office and a package carrier reported they were coughing and had detected an odor that smelled like gas. Firefighters responded and began cordoning off streets around the area. “At first I thought it was freon,” the package carrier said hours later. “But I don’t know how to describe the smell; It was like they had sucked the oxygen out of the place.” The area remained closed for several hours as Vallejo firefighters awaited the county’s HAZMAT team. Emergency crews could not find the source of the problem, recommending that post office officials evaluate their air conditioning units.

Source: [http://www.timesheraldonline.com/news/ci\\_21067378/cough-inducing-odor-forces-evacuation-vallejo-post-office](http://www.timesheraldonline.com/news/ci_21067378/cough-inducing-odor-forces-evacuation-vallejo-post-office)

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

## Agriculture and Food Sector

24. *July 13, Syngenta* – (National) **Kudzu bug is eating through early-planted soybeans.** The kudzu bug is spreading across the South — a migration that could result in significant economic losses for soybean growers, Syngenta reported July 13. Discovered in Georgia in 2009, the kudzu bug has since settled throughout most of Georgia, North and South Carolina, and is now found in parts of Florida, Alabama, Virginia, and Tennessee. While the kudzu bug does feed on kudzu, soybeans have also become a staple in its diet. Kudzu bugs feed on soybeans by sucking nutrients and moisture from the leaves and stems, causing stress, and reducing yields.

Source: <http://www.agprofessional.com/news/Kudzu-bug-is-eating-through-early-planted-soybeans-162221645.html>

25. *July 13, CNN* – (National) **Drought stretches across America, threatens crops.** A severe drought is spreading across the Midwest, resulting in some of the worst conditions in decades and leaving more than 1,000 counties designated as natural disaster areas, authorities said, CNN reported July 13. Farmers in the region are suffering, with pastures for livestock and fields of crops becoming increasingly parched during June, according to the National Climatic Data Center. Many areas in the southern Midwest are reporting the poorest conditions for June since 1988. As of July 10, about 61 percent of the contiguous United States (excluding Alaska, Hawaii, and Puerto Rico) was experiencing drought, the highest percentage in the 12-year record of the U.S. Drought Monitor. Unusually high temperatures and little rainfall have led to “widespread deterioration and expansion of dryness and drought” in the Midwest, northwestern Ohio Valley, and southern Great Plains, the drought monitor said. That has left 1,016 counties in 26 States termed as natural disaster areas, the U.S. Department of Agriculture said the week of July 9. A county is generally qualified as a natural disaster area if it has suffered severe drought for 8 consecutive weeks. The past 12 months have been the warmest the United States has experienced since records began in 1895, the climatic data center said.  
Source: [http://www.cnn.com/2012/07/13/us/midwest-drought/index.html?hpt=hp\\_t1](http://www.cnn.com/2012/07/13/us/midwest-drought/index.html?hpt=hp_t1)
26. *July 13, Associated Press* – (Iowa) **9 counties to get help for spring freeze.** Farmers in some Iowa counties whose crops were affected by a cold snap in April following a warm March may get some help from the U.S. Department of Agriculture (USDA), the Associated Press reported July 13. The USDA Secretary issued disaster declarations to assist farmers in nine counties. The disaster declaration is for Audubon, Chickasaw, Clayton, Delaware, Greene, Harrison, Jackson, Johnson, and Lee.  
Source: <http://www.timesrepublican.com/page/content.detail/id/247186/9-counties-to-get-help-for-spring-freeze-.html?isap=1&nav=5013>

For more stories, see items [11](#), [21](#), [47](#), [50](#),

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

## **Water Sector**

27. *July 12, Mlive.com* – (Michigan) **Bay City plagued by 25 water main breaks from hot weather in less than three weeks.** Recent hot weather put a strain on Bay City, Michigan’s water system, causing 25 water main breaks in less than 3 weeks, Mlive.com reported July 12. “This increase in the number of pipe failures is directly related to high water use in the community and increased water flows related to the recent hot and dry weather,” according to a news release. Since June 24, water main breaks occurred in all areas of the city, according to the City of Bay City Water Distribution Department, with multiple pipe failures on Euclid Avenue. City road crews were making temporary repairs where pavement was dug up for the required pipe repairs, and permanent road repairs will be made later.  
Source: [http://www.mlive.com/news/bay-city/index.ssf/2012/07/bay\\_city\\_plagued\\_by\\_25\\_waterma.html](http://www.mlive.com/news/bay-city/index.ssf/2012/07/bay_city_plagued_by_25_waterma.html)

28. *July 12, Roanoke Times* – (Virginia) **Water main break causing outages, pressure issues for some in Roanoke.** A spokeswoman with the Western Virginia Water Authority said a water main break — not a pump station problem — was affecting water service in Roanoke, Virginia, for far fewer customers than originally announced, the Roanoke Times reported July 12. Homes on Mason Mill Road Northeast could experience reduced pressure or no water while crews fix the break in a 12-inch main, said a water authority spokeswoman. The break should take about 12 hours to fix, she said. Emergency dispatchers in Roanoke and Roanoke County were being told the outage was citywide and could spread to the county late July 12. Hollins Road from Orange Avenue to Masons Mill Road was closed for several hours while crews fixed the break.  
Source: <http://www.roanoke.com/news/breaking/wb/311528>
29. *July 12, WGCL 46 Atlanta* – (Georgia) **Hazmat crews respond to hydrogen peroxide spill at Covington plant.** The Covington, Georgia Fire Department and HAZMAT crews responded to a hydrogen peroxide spill at a water treatment facility July 12. A forklift operator was unloading hydrogen peroxide containers when he lost control and spilled the containers. One employee suffered burns to his ankles and feet. The hydrogen peroxide is a 35 percent concentration and HAZMAT crews were watering it down so it could go into the retention pool outside the plant.  
Source: <http://www.cbsatlanta.com/story/19013857/hazmat-crews-respond-to-hydrogen-peroxide-spill-at-covington-plant>

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

## **Public Health and Healthcare Sector**

30. *July 13, KUSA 9 Denver* – (Colorado) **Denver area oral surgeon may have exposed patients to HIV.** Patients of two Denver area practices were advised to get tested July 12 after a licensed dentist and practicing oral surgeon may have exposed them to HIV, hepatitis B, and/or hepatitis C. The Colorado Department of Public Health and Environment has sent out more than 8,000 letters to patients and former patients of an oral surgeon in Highlands Ranch and Denver. However, the department believes there are more patients that have been impacted. An investigation began after a report of unsafe injection practices. During the investigation, the health department determined syringes and needles used to inject medications through patients' IV lines were saved and reused. The health department advised anyone who was a patient of the oral surgeon in Highlands Ranch and Denver to be tested if they received intravenous medications including sedation from September 1999 through June 2011. Officials said patients may be at risk if they were seen by the surgeon at the following locations: September 1999 to June 2011 - Stein Oral and Facial Surgery, 8671 S. Quebec St., #230, Highlands Ranch, CO 80130; August 2010 to June 2011 at Stein Oral and Facial Surgery (New Image Dental Implant Center), 3737 E.1st Ave., Suite B, Denver, CO 80206.  
Source: <http://www.9news.com/news/local/article/277306/222/Denver-area-dentist-may-have-exposed-patients-to-HIV>

31. *July 13, Dover Fosters Daily Democrat* – (New Hampshire) **Four more Exeter Hospital patients have hep C: Total of 31 cases now.** The number of people who were infected with hepatitis C while being treated at Exeter Hospital in Exeter, New Hampshire, now stands at 30. State health officials announced July 12 that four additional patients have tested positive for the liver disease, joining 26 others who were previously diagnosed. One hospital employee is also carrying the virus, bringing the total number of related cases to 31. The tally has increased steadily since the end of May, when hospital administrators announced the discovery of the first four cases. Since then, the State has launched a large-scale lab testing program to screen more than 1,000 former patients who were potentially exposed. In the announcement, Exeter Hospital officials said they have now completed blood draws for more than 1,000 of the identified patients, and approximately 45 still must have samples taken.  
Source: [http://www.fosters.com/apps/pbcs.dll/article?AID=/20120713/GJNEWS\\_01/707139927](http://www.fosters.com/apps/pbcs.dll/article?AID=/20120713/GJNEWS_01/707139927)
32. *July 12, WWJ 62 Detroit* – (Michigan) **Nitrogen explosion causes scare at New Center One building.** There was a liquid nitrogen canister explosion in a utility room July 12 at Detroit's Henry Ford Medical Center, New Center One. The incident occurred on the eighth floor. About 25 employees and patients in Henry Ford's Department of Dermatology were temporarily evacuated from the building. HAZMAT crews were called to the scene but the substance was deemed not hazardous. According to a statement by medical center officials, the manufacturer of the liquid nitrogen removed the canister and will investigate what caused it to explode. Liquid nitrogen is a cool liquid used to treat skin disorders. Dermatology services at the clinic were canceled for the remainder of the day as a precaution as overexposure to liquid nitrogen fumes. The medical center expected to resume full operations June 13.  
Source: <http://detroit.cbslocal.com/2012/07/12/nitrogen-explosion-causes-scare-at-new-center-one-building/>

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

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

## **Government Facilities Sector**

33. *July 13, Washington Post* – (Washington, D.C.) **President aware of alleged threat toward First Lady, spokesman says.** The U.S. President was notified of the threats a Washington, D.C. police officer is alleged to have made toward the First Lady earlier in the week, a spokesman for the President said July 13. A White House Deputy Press Secretary told reporters the President is “aware” that an officer, who worked as a motorcycle escort for White House officials and other dignitaries, was moved to administrative duty July 11 after he allegedly was overheard making threatening comments about the First Lady. The Washington, D.C. Police chief confirmed July 12 an investigation into “the allegation of inappropriate comments.” The Special Operations Division performs escorts for the first family and other dignitaries.  
Source: <http://www.washingtonpost.com/local/crime/president-obama-aware-of->

[alleged-threat-toward-first-lady-spokesman-says/2012/07/13/gJQA0nM2hW\\_story.html](http://www.gsnmagazine.com/node/26743?c=perimeter_protection)

34. *July 12, Government Security News* – (Florida; North Carolina) **Both political conventions need perimeter protection equipment.** The U.S. Secret Service wants to hire a contractor that can provide all necessary perimeter security equipment — including portable vehicle barriers, anti-scale fencing, and crowd control barricades — which will be used to control crowds and protect dignitaries at the Republican National Convention in Tampa, Florida, and the Democratic National Convention in Charlotte, North Carolina, Government Security News reported July 12. The vendor will provide coordination and management services at both events, which have each been determined to be a National Special Security Event, according to a Secret Service solicitation made public July 11. The GOP convention will take place at Tropicana Field, and the Democratic Convention will occur at Time Warner Cable arena and Bank of America Stadium.  
Source: [http://www.gsnmagazine.com/node/26743?c=perimeter\\_protection](http://www.gsnmagazine.com/node/26743?c=perimeter_protection)

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

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

## Emergency Services Sector

35. *July 13, KFYI 550 AM Phoenix* – (Arizona) **Fumes sicken workers at Mesa 911 center.** A building that serves as the police and fire dispatch center for the city of Mesa, Arizona, was evacuated early July 12 after a strong odor made its way through the building and workers began complaining of feeling ill. According to the Mesa Fire Department, a new generator had been installed in the building recently. During testing, the exhaust pipes of the generator got hot, and paint that covered the exhaust pipes began giving off fumes. Sixty people who work in the building were evacuated. At least 16 people were evaluated by medical personnel on scene, and four were taken to a hospital. The Phoenix Fire Department brought in a large fan that was used to clear the air in the building before employees could be let back in. In addition, air quality tests indicated no toxic fumes inside the building. A Mesa Fire spokesman said there was no interruption in police and fire communications.  
Source: <http://politics.kfyi.com/cc-common/mainheadlines3.html?feed=118695&article=10265488>
36. *July 13, Charleston Daily Mail* – (West Virginia) **Massive storm crashed region's Emergency Alert System.** The Emergency Alert System designed to notify the region's residents of severe weather and chemical plant dangers was knocked out by the June 29 windstorm, Kanawha County, West Virginia executives said, according to the Charleston Daily Mail, July 13. The Kanawha Commission president said it is his understanding the county forwards messages it wants broadcast to the National Weather Service station at Southridge, which operates the system. He said few people could have listened to or seen an emergency broadcast immediately following the June 29 storm because Suddenlink, the dominant cable television provider in the Kanawha

Valley, was knocked out, as were several television stations. AM Radio Station WCHS, a system participant, was knocked out for a short period but went back on air using power from a generator, he said.

Source: <http://www.dailymail.com/News/201207120269>

37. *July 12, Fredericksburg Free Lance-Star* – (Virginia) **Ambulance drugs stolen.** Narcotics and sedatives have been reported stolen from Spotsylvania County, Virginia ambulances for the fourth time this year, despite efforts to prevent thefts, the Fredericksburg Free Lance-Star reported July 12. The weekend of July 7, morphine and Versed went missing from three ambulances at stations at Salem Church and Salem Fields. It is unclear how much of each drug was stolen. The Spotsylvania Sheriff's Office is investigating the thefts. In April and May, Versed, morphine, and other drugs to treat patients were stolen in three incidents at Chancellor-area stations. A Chancellor volunteer said officials believe the thefts occurred July 8. Career personnel reported the missing drugs July 9 during routine equipment inspections, a Spotsylvania spokeswoman said.

Source: <http://blogs.fredericksburg.com/newsdesk/2012/07/12/ambulance-drugs-stolen/>

38. *July 12, Associated Press* – (Massachusetts) **Lowell fire truck catches fire.** Firefighters in Lowell, Massachusetts, found themselves battling a fire involving one of their own vehicles inside one of their own fire stations, the Associated Press reported July 12. The deputy fire chief said the truck caught fire early July 12 inside the Lawrence Street firehouse, causing extensive damage to the engine area and putting the vehicle out of commission at least temporarily. He told the Lowell Sun that the fire appears to be accidental but the cause remains under investigation.

Source:

[http://www.boston.com/news/local/massachusetts/articles/2012/07/12/lowell\\_fire\\_truck\\_catches\\_fire/](http://www.boston.com/news/local/massachusetts/articles/2012/07/12/lowell_fire_truck_catches_fire/)

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

## **Information Technology Sector**

39. *July 13, H Security* – (International) **Yahoo! confirms data breach.** Yahoo! confirmed approximately 450,000 e-mail addresses and passwords from its log-in system were leaked on the Internet. The breach was publicized after a security expert posted about it on Twitter and was initially believed only to concern the Yahoo! Voice service. According to Yahoo!, an “old file” from the Yahoo! Contributor Network content sharing platform was compromised and is the source of the log-in data. The company said only around 5 percent of the leaked 450,000 e-mail address and password combinations have valid passwords. Yahoo! stated it is working on fixing the vulnerability and will change the passwords of affected users as well as notify other companies whose user accounts were affected by the breach. In addition to the 140,000 Yahoo! e-mail addresses, there were over 100,000 Gmail addresses and many from Hotmail and other services.

Source: <http://www.h-online.com/security/news/item/Yahoo-confirms-data-breach-1640148.html>

40. *July 13, H Security* – (International) **Symantec Endpoint Protection causing crashes.** A signature update to Symantec’s Endpoint Protection software led to crashes of Windows XP. The problems with Endpoint Protection, a security package mainly used in the corporate environment, became noticeable by the frequent complaints from users and administrators to the company’s support team and in Symantec’s forums. According to an information page, although Symantec reproduced the problem, it is yet to identify the underlying cause. It has now, though, produced updated signatures to work around the problem.  
Source: <http://www.h-online.com/security/news/item/Symantec-Endpoint-Protection-causing-crashes-1641046.html>
41. *July 13, V3.co.uk* – (International) **Nvidia Developer Zone stung by password pilfering hackers.** Nvidia suspended its developer forum following a suspected data breach that may have compromised user passwords. The service was taken offline July 12, with Nvidia posting a statement saying it is investigating the matter. The company indicated the attack targeted user password information. Nvidia warned users about potential phishing scams using the information, urging forum members to remain wary of suspicious e-mails.  
Source: <http://www.v3.co.uk/v3-uk/news/2191413/nvidia-developer-zone-stung-by-password-pilfering-hackers>
42. *July 13, V3.co.uk* – (International) **Cisco warns users of TelePresence security holes.** Cisco advised customers to update their TelePresence system software and appliances following the release of a series of security fixes. The company issued four software updates designed to address vulnerabilities in various components of the videoconferencing platform. According to Cisco’s advisories, the vulnerable components include the TelePresence Manager, Recording Server, Multipoint Switch, and the TelePresence Immersive Endpoint System. If targeted, the components could be exploited for remote code execution operations.  
Source: <http://www.v3.co.uk/v3-uk/news/2191356/cisco-warns-users-of-telepresence-security-holes>
43. *July 12, IDG News Service* – (International) **Oracle to release 88 security fixes.** Oracle will deliver 88 security fixes July 17 for a wide range of its products, according to a pre-release announcement posted to its Web site July 12. A number of the bugs affect more than one product, and customers are advised to apply the patches as soon as possible, Oracle said. Four fixes are for Oracle’s database. Three of the database vulnerabilities involved can be exploited by an attacker over a network without the need for log-in credentials, according to the notice. Oracle is also set to release 22 patches for its Fusion Middleware family, 8 of which can be remotely exploited without a username or password, Oracle said. The company uses the Common Vulnerability Scoring System (CVSS) to rank the seriousness of its patches. One of the fixes, for the Fusion Middleware product JRockit, has a CVSS score of 10.0, the highest on the scale. Another 25 fixes cover weaknesses in Oracle’s Sun product family, including the GlassFish application server and Solaris OS. The patch batch will also deliver six fixes for the MySQL database. None of the weaknesses involved can be exploited remotely without credentials, Oracle said. Other patches in the release include

ones for Hyperion, Enterprise Manager Grid Control, E-Business Suite, Siebel CRM, PeopleSoft, and Oracle Industry Applications.

Source:

[http://www.computerworld.com/s/article/9229081/Oracle\\_to\\_release\\_88\\_security\\_fixes](http://www.computerworld.com/s/article/9229081/Oracle_to_release_88_security_fixes)

44. *July 12, Threatpost* – (International) **AndroidForums.com hacked, user credentials stolen.** An online forum for Android fans and developers was compromised and user account details stolen, according to a notice posted online July 10. Phandroid.com, which operates Androidforums.com, told users that hackers breached a back end database that powers Androidforums.com, an online bulletin board for Android users and developers. The data contained in that database includes androidforums usernames, email addresses, hashed passwords, the IP addresses members registered with, and forum group memberships, among other data. Phandroid.com believes the attack was aimed at gathering e-mail addresses for spam runs.

Source: [http://threatpost.com/en\\_us/blogs/androidforumscom-hacked-user-credentials-stolen-071212](http://threatpost.com/en_us/blogs/androidforumscom-hacked-user-credentials-stolen-071212)

45. *July 12, ZDNet* – (International) **Microsoft patches Windows Live identity theft flaw.** Two security researchers recently discovered a serious vulnerability in Microsoft's Windows Live service. The cross-site scripting (XSS) flaw means an attacker could impersonate a Windows Live user by gaining full control of the victim's cookies. Combined with social engineering, this technique could be used to steal a victim's Windows Live identity.

Source: <http://www.zdnet.com/microsoft-patches-windows-live-identity-theft-flaw-7000000832/>

For more stories, see items [4](#), [10](#), [11](#), and [51](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [sos@us-cert.gov](mailto: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

See items [36](#), [39](#), and [45](#)

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



## Commercial Facilities Sector

46. *July 13, Manchester Union Leader* – (New Hampshire) **Propane leak prompts evacuation at Wolfeboro inn.** A leak from a propane gas tank led to evacuation of a downtown inn in Wolfeboro, New Hampshire, July 12. The Wolfeboro Fire-Rescue deputy chief said no one was injured, but the inn was evacuated and North Main Street was closed for a time. First arriving crews found an active leak from one of two 500-gallon propane tanks behind the inn. The inn was evacuated and a hose stream was directed at the tank to cool it. A water supply hose was laid across North Main Street from a nearby hydrant, and the road was shut down for just over 1 hour. Technical assistance was received from Eastern Propane. Inn staff reopened the inn later July 12. Source: <http://www.unionleader.com/article/20120712/NEWS07/707139968>
47. *July 13, Associated Press* – (Texas) **CDC says tea poisoned at Texas restaurant rare.** Health officials said the first known victims of sodium azide poisoning at a public place were hospitalized after drinking tea laced with the chemical at a Dallas-area restaurant 2 years ago, the Associated Press reported July 13. Authorities said the toxic industrial chemical was deliberately added to a tea urn at the Potbelly sandwich shop in Richardson, Texas, when employees were not looking. The five victims of the April 2010 poisoning recovered. The Centers for Disease Control and Prevention said it was “the first detailed report of sodium azide poisonings at a public venue.” A UT-Southwestern Medical Center at Dallas toxicologist who investigated the case said there were no related incidents. Potbelly told the Dallas Morning News they installed tamper-resistant covers on their tea urns. Source: <http://lubbockonline.com/texas/2012-07-13/cdc-says-tea-poisoned-texas-restaurant-rare#.UAA01pFnUSZ>
48. *July 13, WUSA 9 Washington D.C.* – (Maryland) **Residents rescued from flaming Silver Spring apartment building.** Firefighters from Montgomery County, Maryland, fought a three alarm fire in an apartment building in Burtonsville, and officials confirmed some residents were rescued from the fire. A spokesman for Montgomery County Fire and Rescue said fire crews were alerted to the fire July 13. Firefighters arrived on the scene and found the entire building on fire. Officials said 34 units were damaged in the fire that displaced 74 residents in total. Officials said three or four people were rescued from the upper floors of the apartment building. Firefighters evacuated the structure after it became too dangerous for them to fight. Firefighters performed an exterior attack on the building and sprayed it with hoses from ladders. Source: <http://washington.cbslocal.com/2012/07/13/residents-rescued-from-flaming-silver-spring-apartment-building-fire-ensues/>
49. *July 12, KTVX 4 Salt Lake City* – (Utah) **One dead, 3 injured in explosion at Alpine art center.** Fire and emergency crews responded to reports of a boiler explosion at the Alpine Art Center in Utah County, Utah, July 12. One person was confirmed dead, while three others were seriously injured. The explosion happened at the Adonis Bronze factory, which is located inside the Alpine Art Center. The nature of the injuries to the other three people was reported as being burns. Officials said a worker at the bronze business operated a kiln and dipped a sculpture into a nearby boiler when the

explosion happened. The explosion prompted the evacuation of the bronze business employees as well as a luncheon going on nearby. Police, fire, and Occupational Safety and Health Administration investigators looked into the cause of the explosion, which also caused some structural damage at the facility.

Source: <http://www.abc4.com/content/news/slc/story/One-dead-3-injured-in-explosion-at-Alpine-art/zpUKRbptl0a2p8MoP9AXaQ.cspX>

50. *July 12, KMGH 7 Denver* – (Colorado) **Welders working where strip mall fire started.** Welders were working in the area of a strip mall building where a fire ignited at the Denver Tech Center in Denver July 12. The fire began in the Marina Square Strip Mall and witnesses said the blaze burned through the roof of Pho Saigon Le restaurant. A Denver fire spokesman said at one point there was a partial roof collapse and firefighters were pulled from the roof of the building and its interior. Four businesses in the strip mall were evacuated. Fire crews eventually got ahead of the blaze and had it controlled later July 12. The fire burned through the attic. Pho Saigon Le restaurant, Dependable Cleaners, Soundings audio/video store, and Which Wich sandwich company remained closed July 12 while restoration crews placed plywood over the holes that firefighters cut in the roof.

Source: <http://www.thedenverchannel.com/news/31268776/detail.html>

51. *July 12, Ars Technica* – (International) **More user passwords dumped, this time from alleged Billabong.com hack.** Hackers dumped a huge cache of stolen passwords, exposing what they said were as many 35,000 plaintext passcodes from the Web site of clothing maker Billabong International. A post on CodePaste.net claimed 20,000 to 35,000 user names and corresponding passwords were retrieved in the hack of billabong.com. However, the post included only 1,435 plain-text user credentials. The post also included what it claimed were user names and hashed passwords for MySQL accounts used to administer the site. The hackers behind the latest dump suggested they may have gained root access to the Billabong servers. The privileged access would have given them unfettered privileges to read, write, or delete files or install new applications.

Source: <http://arstechnica.com/security/2012/07/user-passwords-dumped-in-alleged-billabong-com-hack/>

For more stories, see items [34](#)

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

## **National Monuments and Icons Sector**

52. *July 13, Redding Record-Searchlight* – (California) **Flat Fire in Trinity County grows to 874 acres with 20 percent containment.** The Flat Fire 30 miles west of Weaverville in Trinity County, California, had charred 874 acres of forest and was 20 percent contained as of July 13, U.S. Forest Service officials said. Meanwhile, crews in the Mendocino National Forest continue to battle the Mill Fire, which had grown to more than 23,000 acres. That blaze was 45 percent contained, though officials did not expect full containment until the week of July 16. The Flat Fire, which started July 11 at the

Hayden Flat campground inside Shasta-Trinity National Forest, spread toward Weaverville between a northern ridge and Highway 299, said a spokeswoman for the Forest Service. The fire had not jumped Highway 299. “If it jumps any of the major drainages, there could be problems,” she said. The fire had grown to about 500 acres, said a public affairs officer for the Shasta-Trinity National Forest. Firefighters farther south in the Mendocino National Forest were battling the much larger Mill Fire, which had burned 17,300 acres by July 12, according to the Forest Service. More than 1,500 people are battling that blaze, which broke out the week of July 9. It had cost \$5 million in damage and suppression, officials said.

Source: <http://www.redding.com/news/2012/jul/13/flat-fire-in-trinity-county-grows-to-640-acres/>

53. *July 13, Associated Press* – (Idaho; Oregon) **Wildfires keep southern Idaho fire crews busy.** The Avelene Fire, burning in a section of the Boise National Forest about 25 miles northeast of Boise, Idaho, scorched 210 acres so far and was responsible for the evacuation of nearby homes, the Associated Press reported July 13. The fire was one of a handful of fires in southwestern Idaho and eastern Oregon responsible for the thin veil of smoke hovering above the Boise area, prompting State health officials July 12 to downgrade the air quality rating for the Treasure Valley. The voluntary evacuation order issued July 11 remained in effect. Fire managers hoped to have the fire contained by July 13. More than 150 firefighters were battling the C Fire burning 10 miles east of Donnelly. The fire was 30 percent contained. Firefighters also gained the upper hand on the Kinyon Road Fire, which flared up July 7 and so far has burned more than 367 square miles of grass and sagebrush near the south-central town of Castleford, making it the biggest blaze in Idaho so far this year. A fire spokesman said the fire is 90 percent contained, with full containment expected later July 12.

Source: [http://www.idahopress.com/news/state/wildfires-keep-southern-idaho-fire-crews-busy/article\\_f670f94c-cca7-11e1-99cc-001a4bcf887a.html](http://www.idahopress.com/news/state/wildfires-keep-southern-idaho-fire-crews-busy/article_f670f94c-cca7-11e1-99cc-001a4bcf887a.html)

54. *July 12, KFFB 5 Great Falls* – (Montana) **Wildfire breaks out in Bob Marshall wilderness.** The U.S. Forest Service said a wildfire has broken out in the Bob Marshall Wilderness northwest of Augusta, Montana. A Lewis and Clark National Forest spokesman said the fire was reported July 12 and had grown to 200 acres within a few hours. Even though it was burning in a wilderness area, he said firefighters were responding quickly because of the potential for rapid growth. Elsewhere, an uncontained fire in southwestern Montana on the Idaho line grew to 2 square miles. Officials managing a complex of five large wildfires in southeastern Montana said containment lines were holding in red-flag weather conditions.

Source: <http://www.kfbb.com/news/local/Wildfire-breaks-out-in-Bob-Marshall-Wilderness-162316936.html>

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

## **Dams Sector**

Nothing to report

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



**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 <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703)387-2314
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.