



Daily Open Source Infrastructure Report 18 November 2014

Top Stories

- The U.S. Chemical Safety Board and the Occupational Safety and Health Administration are investigating a methyl mercaptan leak at a DuPont and Co. plant in LaPorte, Texas, that killed four workers and injured one November 15.– *Reuters* (See item [3](#))
- A boil water advisory was issued for customers in Sussex Borough November 16 until November 21 following the restoration of water service after a November 13 water main break during construction work on Route 23 in which over 1 million gallons of water was lost. – *New Jersey Herald* (See item [19](#))
- The Dickson County Sheriff's Office in Tennessee's computer system was compromised by the CryptoWall ransomware in October after an employee clicked on a malicious advertisement that forced staff into paying \$500 in digital currency in order to retrieve 72,000 files.– *Softpedia* (See item [26](#))
- Eight people were injured and 40 Ohio University students in Athens, Ohio, were displaced after a major fire damaged 6 buildings that included university housing and shut off power to the affected area for several hours November 16. – *Athens News* (See item [40](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *November 13, U.S. Attorney's Office, Northern District of Ohio* – (Ohio) **Stow man charged with cyber crimes.** Authorities unsealed a federal indictment November 13 charging an Ohio man for attempting to install malware on the computer systems of Eaton Corporation while he was employed as a contracted financial analyst in May. The malicious code was discovered after the suspect disclosed its existence to a former coworker.
Source: <http://www.fbi.gov/cleveland/press-releases/2014/stow-man-charged-with-cyber-crimes>
2. *November 13, Los Angeles Times* – (West Virginia) **Former Massey Energy chief executive indicted in 2010 mine explosion.** A West Virginia grand jury charged the former chief executive of Massey Energy Co., November 12 for his role in conspiring to violate federal mine safety standards and impeding federal mine safety officials at the company's Upper Big Branch mine following an April 2010 coal mine explosion that killed 29 people.
Source: <http://www.latimes.com/nation/nationnow/la-na-nn-massey-energy-don-blankenship-20141113-story.html>

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

Chemical Industry Sector

3. *November 16, Reuters* – (Texas) **Federal agencies to begin probe of DuPont Texas plant deaths.** The U.S. Chemical Safety Board and the Occupational Safety and Health Administration are investigating following a methyl mercaptan leak at a DuPont and Co. plant in LaPorte, Texas, November 15 that killed four workers. A fifth employee was transported to an area hospital with injuries.
Source: <http://www.reuters.com/article/2014/11/17/us-usa-chemicals-death-idUSKCN0J00XA20141117>
4. *November 14, Joliet Herald News* – (Illinois) **Another chemical leak at Stepan plant.** Crews worked November 14 to contain a vapor leak of sulfur trioxide from a railcar at the Stepan Company plant in Elwood which lasted about 13 hours. The November 14 release and a November 13 leak from a separate railcar at the same facility are under investigation, while crews were scheduled to make repairs November 15.
Source: <http://www.theherald-news.com/2014/11/14/another-chemical-leak-at-stepan-plant/ayvq04u/>

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

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

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

Critical Manufacturing Sector

5. *November 14, Detroit News* – (National) **Ford expands Ranger Takata air bag recall.** Ford announced that it is expanding a previous recall of 25,000 model year 2004-2005 Ranger vehicles to include both passenger and driver airbags manufactured by Takata. The airbag inflators can explode during deployment, sending metal fragments into the vehicle cabin.
Source: <http://www.detroitnews.com/story/business/autos/ford/2014/11/14/ford-expands-ranger-takata-air-bag-recall/19050797/>

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

Defense Industrial Base Sector

Nothing to report

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

Financial Services Sector

6. *November 14, Baltimore Sun* – (New York; Maryland) **Former owner of Empire Towers indicted in \$7million fraud.** The U.S. Securities and Exchange Commission filed a complaint November 14 against a Hampton Bays, New York man who owned the Empire Towers building in Glen Burnie, Maryland, for allegedly raising over \$7 million from investors by selling fraudulent, unregistered bonds. The SEC also charged the man's investment advisor for allegedly participating in the scheme.
Source: <http://www.baltimoresun.com/news/maryland/anne-arundel/bs-md-aa-empire-towers-owner-indicted-20141114-story.html>

For another story, see item [32](#)

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

Transportation Systems Sector

7. *November 17, KNBC 4 Los Angeles* – (California) **“Dangerous Device” found in truck on I-5, driver arrested** Authorities shut down several lanes on Interstate 5 south near the Interstate 805 merger in Del Mar Heights for 4 hours November 16 while a bomb squad disposed of an explosive device after it was discovered in the vehicle of a drunken driver during a search and arrest.
Source: <http://www.nbclosangeles.com/news/california/Explosive-Device-Team-Blocking-I-5-Freeway-282865111.html>
8. *November 16, Associated Press* – (New Jersey) **Bus, military vehicle crash injures several people.** Several people were injured when a military vehicle collided with a New Jersey Transit Bus on northbound lanes of the New Jersey Turnpike near

Interchange 14 in Newark November 16. Authorities are investigating the accident.
Source: <http://www.nbc40.net/story/27399104/bus-military-vehicle-crash-injures-several-people>

9. *November 16, KPIX 5 San Francisco; San Francisco Bay City News* – (California) **Woman dies after being struck in hit-run collision on Highway 29 near Calistoga.** A fatal hit-and-run collision killed one woman and forced the closure of State Highway 29 in Napa County nearly 11 hours while authorities investigated a potential homicide.
Source: <http://sanfrancisco.cbslocal.com/2014/11/16/fatal-hit-and-run-crash-closes-highway-29-near-calistoga/>
10. *November 14, Richmond Times-Dispatch* – (Virginia) **Driver seriously injured in state Route 288 cement mixer crash.** The northbound lane of Route 288 near Chesterfield was shut down for approximately 4 hours November 14 after a cement truck overturned when a tire blew out. The driver suffered serious injuries and was transported to a local hospital.
Source: http://www.timesdispatch.com/news/local/traffic/driver-seriously-injured-in-state-route-cement-mixer-crash/article_edf81c45-3513-577f-99ea-558865b66d7e.html
11. *November 14, Associated Press* – (California) **Seattle-bound flight diverted after bird strike.** An Alaska Airlines flight en route to Seattle from Oakland, California, returned to Oakland shortly after takeoff due to a bird strike November 14. The plane is being inspected and kept in Oakland.
Source: <http://mynorthwest.com/174/2644507/Seattlebound-flight-diverted-after-bird-strike>
12. *November 14, Waco Tribune-Herald* – (Texas) **Northbound I-35E reopened after Waxahachie-area semi crash.** Northbound lanes of Interstate 35 East near Waxahachie were closed for more than 8 hours after 2 jackknifed semi-trucks crashed near Ganaway Bridge November 14.
Source: http://www.wacotrib.com/news/traffic/northbound-i--e-reopened-after-waxahachie-area-semi-crash/article_cf08ab00-c859-5a0a-8179-dae848a47e0a.html

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

Food and Agriculture Sector

13. *November 15, Hanover Evening Sun* – (Pennsylvania) **Damage from Pa. sawmill fire hits \$800K.** Authorities are investigating the cause of a 2-alarm fire at a Menallen Township sawmill November 13 that resulted in a structure collapse and caused an estimated \$800,000 in damage. The sawmill resumed most operations November 14.
Source: <http://www.firehouse.com/news/11775047/two-alarm-blaze-at-menallen-township-sawmill-costly>
14. *November 15, U.S. Food and Drug Administration* – (National) **Lundberg Family Farms recalls Eco-Farmed and Organic Brown Rice Flour because of possible health risk.** The U.S. Food and Drug Administration announced November 14 that

Lundberg Family Farms issued a recall for specific bags of its Eco-Farmed Brown Rice Flour and Organic Brown Rice Flour due to possible Salmonella contamination. The products were distributed in retail store bulk bins and 25-pound bulk bags between November 4 and November 12 in five States and via mail order.

Source: <http://www.fda.gov/Safety/Recalls/ucm423223.htm>

15. *November 15, U.S. Department of Agriculture* – (National) **Pennsylvania firm recalls Pretzel Dog products due to misbranding and undeclared allergens.** The Food Safety and Inspection Service announced November 15 that City Line Foods Manufacturing Co. recalled about 1,196,669 pounds of frozen pretzel hot dog products due to undeclared soy lecithin caused by misbranding. The products were shipped nationwide for retail distribution and fundraising.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2014/recall-079-2014-release>
16. *November 14, U.S. Food and Drug Administration* – (National) **Great American Appetizers, Inc. recalls HyVee Mozzarella Cheese Sticks due to undeclared soy flour, yellow #5, and yellow #6.** The U.S. Food and Drug Administration reported November 14 that Great American Appetizers, Inc. recalled 662 cases of HyVee Mozzarella Cheese Sticks due to undeclared soy flour, yellow #5, and yellow #6. The products were sold in 8-ounce cartons and distributed to retailers in several States.
Source: <http://www.fda.gov/Safety/Recalls/ucm423211.htm>
17. *November 14, U.S. Food and Drug Administration* – (National) **B&G Foods issues allergy alert on undeclared peanut and almond in product.** The U.S. Food and Drug Administration reported that B&G Foods announced November 14 a recall for certain Ortega and Las Palmas-branded taco season, sauce, and kit products after a third party supplier informed the company that one or more of the ingredients used in the affected items contain peanuts and almonds that were not declared. The products were distributed to retailers and foodservice outlets nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm423216.htm>
18. *November 14, U.S. Department of Agriculture* – (National) **Illinois firm recalls pierogi products due to misbranding and undeclared allergens.** The Food Safety and Inspection Service announced November 14 that Kasia's Deli Inc. issued a recall for about 2,059 pounds of Polana pierogi products due to undeclared wheat, soy, eggs, and milk caused by misbranding. The affected products were produced before September 19 and distributed nationwide via online sales.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2014/recall-078-2014-release>

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

Water and Wastewater Systems Sector

19. *November 16, New Jersey Herald* – (New Jersey) **Customers in Sussex advised to continue boiling water.** A boil water advisory was issued for customers in Sussex

Borough November 16 until November 21 following the restoration of water service after a November 13 water main break during construction work on Route 23. The water system lost over 1 million gallons of water due to the break and crews continue work to bring the borough's upper water tank to full capacity.

Source: <http://www.njherald.com/story/27399965/customers-in-sussex-advised-to-continue-boiling-water>

20. *November 16, Wilkes-Barre Times Leader* – (Pennsylvania) **Pennsylvania American Water lifts boil advisory.** A boil water advisory was lifted for Pennsylvania American Water customers in Luzerne, Swoyersville, Pringle, and West Wyoming November 16 after acceptable bacteria test results were obtained from samples collected following the November 13 issuance of the advisory.

Source: <http://www.timesleader.com/news/local-news/50696554/Pennsylvania-American-Water-lifts-boil-advisory>

21. *November 15, WTAJ 10 Altoona* – (Pennsylvania) **Boil water advisory in effect.** Officials issued a boil water advisory to residents in Driftwood Borough November 15 until further notice because of the potential for bacteria contamination due to low pressure as a result of recent water leaks in the distribution system.

Source: <http://www.wearecentralpa.com/story/d/story/boil-water-advisory-in-effect/13046/L4Xdcx4sLU-WqRK3HOPUwA>

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

Healthcare and Public Health Sector

Nothing to report

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

Government Facilities Sector

22. *November 16, KGBT 4 Harlingen* – (Texas) **City trucks stolen, three ambulances burglarized in Weslaco.** Authorities are searching for the suspects responsible for breaking into a public facilities building in Weslaco November 14 and stealing city trucks, tool parts and supplies from three ambulances. Police recovered the two trucks in separate locations.

Source: <http://www.valleycentral.com/news/story.aspx?id=1123753>

23. *November 14, KING 5 Seattle* – (Washington) **Seattle Public Schools security breach impacts thousands of students.** Seattle Public Schools notified the parents of at least 8,000 special education students November 13 of a November 11 security breach involving the private and personal information of their children including names, student identification numbers, and disabilities after a law firm retained by the district inadvertently sent the information to an individual involved in an ongoing case.

Source: <http://www.king5.com/story/news/local/seattle/2014/11/14/seattle-public-schools-admits-to-security-breach-impacting-thousands-of-students/19012537/>

For another story, see item [36](#)

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

Emergency Services Sector

24. *November 17, Charlotte Observer* – (North Carolina) **Richmond County prison searching for two escaped inmates who have ties to Rowan, McDowell counties.** Correctional authorities are searching for two inmates who escaped from the Morrison Correctional minimum unit in Richmond County, North Carolina, by allegedly jumping over the fence November 16.
Source: <http://www.charlotteobserver.com/2014/11/17/5321887/richmond-county-prison-searching.html>
25. *November 15, San Francisco Bay City News* – (California) **3 sheriff's employees charged with smuggling cellphones, drugs into jail.** A sheriff's deputy and two correctional officers at the San Mateo County Maguire Main Jail in Redwood City were arrested and charged November 13 for allegedly smuggling drugs and cellphones to a known gang member following an independent investigation.
Source: <http://www.nbcbayarea.com/news/local/3-Sheriffs-Employees-Charged-With-Smuggling-Cellphones-Drugs-Into-Jail-282768921.html>
26. *November 14, Softpedia* – (Tennessee) **Sheriff's office pays ransom to unlock files encrypted by CryptoWall.** The sheriff's office in Dickson County, Tennessee, reported that its computer system was the victim of the CryptoWall ransomware in October after an employee clicked on a malicious advertisement placed on the Web site of a local radio station. The sheriff's office was forced to pay about \$500 in digital currency in order to retrieve 72,000 files that were encrypted by the ransom-demanding malware.
Source: <http://news.softpedia.com/news/Sheriff-s-Office-Pays-Ransom-to-Unlock-Files-Encrypted-by-CryptoWall-464962.shtml>

For additional stories, see items [22](#) and [36](#)

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

Information Technology Sector

27. *November 17, Softpedia* – (International) **BusyBox devices compromised through Shellshock attack.** Researchers with Trend Micro identified a new version of the Bashlite malware that identifies devices on an infected system's network that use the BusyBox software for Linux, including routers, and can then attempt to compromise them using the Shellshock vulnerability.
Source: <http://news.softpedia.com/news/BusyBox-Devices-Compromised-Through-Shellshock-Attack-465087.shtml>
28. *November 17, Softpedia* – (International) **Steam password stealer is stored on Google**

- Drive.** A researcher with Panda Security analyzed and reported a piece of malware designed to steal passwords for the Steam gaming service that is being delivered from a Google Drive account. The account was still active when the researcher reported the malware November 16 and targets victims via a fraudulent link in Steam chat that downloads an executable file.
Source: <http://news.softpedia.com/news/Steam-Password-Stealer-Is-Stored-On-Google-Drive-465107.shtml>
29. *November 17, The Register* – (International) **WinShock PoC clocked: But DON'T PANIC... It's no Heartbleed.** Researchers released a proof-of-concept (PoC) exploit for a SChannel crypto library flaw that was patched the week of November 10 in a Microsoft patch release. The flaw can still be exploited in unpatched Windows Server 2012, 2008 R2, and 2003 installations to run arbitrary code.
Source: http://www.theregister.co.uk/2014/11/17/ms_schannel_crypto_poc/
30. *November 17, The Register* – (International) **Attack reveals 81 percent of Tor users but admins call for calm.** A paper released by researchers at the Indraprastha Institute of Information Technology outlined a traffic confirmation attack method that the researchers stated could be used to identify users of the Tor anonymity network in 81 percent of cases if an attacker has sufficient resources.
Source: http://www.theregister.co.uk/2014/11/17/deanonymization_techniques_for_tor_and_bitcoin/
31. *November 17, Securityweek* – (International) **Alleged creators of WireLurker malware arrested in China.** Authorities in China arrested three individuals for allegedly creating and distributing the WireLurker malware targeting Mac OS X, iOS, and Windows devices and shut down the Web site used to distribute the malware.
Source: <http://www.securityweek.com/alleged-creators-wirelurker-malware-arrested-china>
32. *November 17, Securityweek* – (International) **Majority of top 100 paid iOS, Android apps have hacked versions: Report.** Arxan Technologies released their annual State of Mobile App Security report which found that there were cloned or repackaged versions of 97 percent of the top 100 paid Android apps and 87 percent for top 100 paid iOS apps, and that repackaged or cloned financial services apps existed for 95 percent of apps on Android and 70 percent in iOS, among other findings.
Source: <http://www.securityweek.com/majority-top-100-paid-ios-android-apps-have-hacked-versions-report>
33. *November 16, Softpedia* – (International) **New variant of Dofail trojan emerges with strong evasion features.** Fortinet researchers identified a new variant of the Dofail botnet malware that contains several changes aimed at preventing the malware from being detected and analyzed.
Source: <http://news.softpedia.com/news/New-Variant-of-Dofail-Trojan-Emerges-with-Strong-Evasion-Features-465050.shtml>

34. *November 15, Softpedia* – (International) **New encryption ransomware offers file decryption trial.** Researchers at Webroot identified a new piece of encryption ransomware dubbed CoinVault that encrypts victims' files using AES-256 encryption, demands a ransom, and offers a free trial of the decryption performed if a ransom is paid.
Source: <http://news.softpedia.com/news/New-Encryption-Ransomware-Offers-File-Decryption-Trial-465027.shtml>
35. *November 14, Softpedia* – (International) **Google misses trojan SMS app in Play Store for more than a year.** An SMS trojan named Thai Fun Content was identified by Malwarebytes researchers on the Google Play Store and was available for download for over 1 year. The app subscribes victims to a paid SMS service and charges victims \$0.37 per day.
Source: <http://news.softpedia.com/news/Google-Misses-Trojan-SMS-App-in-Play-Store-for-More-than-a-Year-465005.shtml>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@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: <http://www.it-isac.org>

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

Communications Sector

36. *November 14, McDowell News* – (North Carolina) **Phone outage impacts 17,500 customers.** Around 17,500 residents, businesses, and public agencies were without landline and cell phone service for nearly 4 hours November 13 after a fiber optic line was severed on U.S. 70 west in Pleasant Gardens. Emergency 9-1-1 service calls were also impacted during the outage.
Source: http://www.mcdowellnews.com/news/phone-outage-impacts-customers/article_ee66dd52-6c41-11e4-b85d-b7d2a99636bc.html

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

Commercial Facilities Sector

37. *November 17, Dallas Morning News* – (Texas) **About two dozen residents displaced early Monday after a fire at an Irving apartment complex.** A 2-alarm fire at the Shadows of Cottonwood Apartments in Irving November 17 displaced about 30 residents and damaged 12 apartment units. The cause of the blaze is under investigation.
Source: <http://thescoopblog.dallasnews.com/2014/11/about-two-dozen-residents-displaced-early-monday-after-a-fire-at-an-irving-apartment-complex.html/>

38. *November 17, Associated Press* – (Ohio) **Off-duty police officer fatally shot at Ohio pub.** Police arrested and charged a suspect November 16 for allegedly opening fire inside Papa Don's Pub in Akron when he returned to the restaurant after being asked by management to leave due to his unruly behavior. An off-duty police officer was killed when he approached the suspect who brandished a gun and shot and injured 4 additional patrons.
Source: <http://www.seattlepi.com/news/crime/article/Off-duty-police-officer-fatally-shot-at-Ohio-pub-5897006.php>
39. *November 16, KXTV 10 Sacramento* – (California) **Two-alarm strip mall fire ruled arson.** A 2-alarm fire that broke out November 15 at a Sacramento County strip mall engulfed two structures and caused between \$100,000 and \$200,000 in damage. Arson investigators ruled the fire as incendiary in nature.
Source: <http://www.news10.net/story/news/local/arden-lariviera/2014/11/15/two-alarm-sacramento-fire/19084315/>
40. *November 16, Athens News* – (Ohio) **Blaze heavily damages block of uptown buildings.** Authorities are investigating the cause of a November 16 fire that damaged 6 businesses in Athens, Ohio, and injured 8 individuals, including 3 firefighters and 1 police officer. At least 40 students were displaced from apartment units located above the affected businesses, and a subsequent power outage affected the area for several hours.
Source: <http://www.athensnews.com/ohio/article-43673-blaze-heavily-damages-block-of-uptown-buildings.html>
41. *November 15, MyNorthwest.com* – (Washington) **Gas leak prompts evacuation at Lynnwood Costco.** Hundreds of patrons and staff were evacuated from a Costco store in Lynwood November 15 after a refrigerant line ruptured and released a visible cloud of gas. One individual was transferred to an area hospital with injuries after he came in direct contact with the gas.
Source: <http://mynorthwest.com/11/2645018/Gas-leak-prompts-evacuation-at-Lynnwood-Costco>
42. *November 14, Suffolk County Newsday* – (New York) **Water main break causes 9-hour closing of Merrick Road in Bellmore.** About 20 commercial businesses in Nassau County were without water service for nearly 9 hours November 14 following a break in a 12 inch water main that flooded the area.
Source: <http://www.newsday.com/long-island/nassau/merrick-road-intersection-in-bellmore-closed-for-9-hours-due-to-water-main-break-cops-say-1.9617483>

For another story, see item [36](#)

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

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 10 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) 942-8590
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@hq.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.