Daily Open Source Infrastructure Report
20 January 2016

Top Stories

- Southern California Gas Company announced January 18 that a natural gas leak at the Aliso Canyon facility in Los Angeles, which has released methane since October 2015, will be capped by the end of February. – *KNBC 4 Los Angeles* (See item **1**)
- Authorities are investigating after vandals opened 20 water lines and drained approximately 400,000 gallons of drinking water in Flagler County, Florida, January 18. – *Associated Press* (See item **19**)
- The U.S. President declared a state of emergency in Michigan in response to lead-contaminated drinking water in the city of Flint. – *San Antonio Post* (See item **20**)
- A researcher from Perception Point discovered a new wild zero-day vulnerability affecting Android phones running 4.4 KitKat operating system (OS) and Linux machines running Kernel 3.8 or higher OS that allows attackers to delete files among other issues. – *CSO Online* (See item **30**)

Fast Jump Menu

Energy Sector

1. *January 18, KNBC 4 Los Angeles* – (California) **Porter Ranch gas leak will be stopped by end of February, utility says.** Southern California Gas Company announced January 18 that a natural gas leak at the Aliso Canyon facility that has been releasing methane since October 2015 forcing officials to place the Porter Ranch section of Los Angeles, under a state of emergency will be capped by the end of February with help from a relief well project.
Source: http://www.nbclosangeles.com/news/local/Porter-Ranch-Gas-Leak-Cap-Well-365714041.html

2. *January 16, Salt Lake City Deseret News* – (Utah) **Interior Department halts new federal coal leases.** The U.S. Department of the Interior announced January 15 that it is halting the issuance of any new Federal coal leases under the Federal coal program in Utah for 3 years due to concerns raised by the U.S. Government Accountability Office regarding pollution, resources, and public health impacts of coal mining.
Source: http://www.deseretnews.com/article/865645582/Interior-Department-halts-new-federal-coal-leases.html?pg=all

Chemical Industry Sector

3. *January 16, KTRK 13 Houston* – (Texas) **1 dead, 3 injured after chemical tank explosion in Pasadena.** A chemical tank explosion at PeroxyChem plant in Pasadena killed 1 person and injured 3 others January 16 after a contractor's equipment exploded during a routine function, causing a rupture and chemical spill. The incident is under investigation.
Source: http://abc13.com/news/1-dead-4-injured-after-chemical-tank-explosion-in-pasadena/1161670/

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *January 16, Fairfield-Suisun City Daily Republic* – (California) **2 from Solano County plead guilty in multimillion-dollar mortgage fraud scheme.** Prosecutors announced January 16 that two Solano County, California residents pleaded guilty January 15 to conspiracy to make false statements on loan applications after the two reportedly took

part in a $10 million loan fraud scheme by convincing homeowners facing foreclosure to sign the titles of their homes over to the pair's business, Capital Access LLC where they would sell the titles to straw buyers, who obtained loans under the false pretense that they would reside in the houses. The company stripped home equity from at least 69 properties in California to pay the operating expenses of Capital Access LLC.
Source: http://www.dailyrepublic.com/news/fairfield/2-from-solano-county-plead-guilty-in-multimillion-dollar-mortgage-fraud-scheme/

Transportation Systems Sector

5. *January 19, WWJ 62 Detroit* – (Michigan) **US-23 to be closed for hours after semi rolls over, spills milk across road.** The northbound lanes of US-23 in Fenton, Michigan, were closed for several hours January 19 while crews worked to clear the wreckage from an overturned semi-truck that spilled milk and oil.
Source: http://detroit.cbslocal.com/2016/01/19/us-23-to-be-closed-for-hours-after-semi-carrying-milk-rolls-over/

6. *January 18, WAVY 10 Portsmouth* – (Virginia) **Passengers upset over delays after plane makes emergency landing.** A United Airlines flight en route to the Dominican Republic from Newark, New Jersey, was forced to make an emergency landing at Norfolk International Airport in Virginia January 17 due to a mechanical issue in the right engine. The airline attempted to re-accommodate passengers on another flight January 18.
Source: http://wavy.com/2016/01/17/boeing-757-makes-emergency-landing-at-norfolk-airport/

7. *January 18, Santa Barbara Noozhawk* – (California) **1 dead after truck, Chumash bus collide on Highway 154.** A portion of Highway 154 near Los Olivos was closed for more than 2 hours January 18 after a Chumash Casino passenger bus and another vehicle collided head-on leaving 1 person dead.
Source:
http://www.noozhawk.com/article/bus_truck_crash_reported_on_highway_154_near_zaca_station_road

8. *January 17, KRON 4 San Francisco* – (California) **One person dead in a fatal car accident on Highway 4 in Martinez.** All lanes of Highway 4 in Martinez, California were closed for more than 2 hours January 16 while officials investigated the scene of a fatal 3-vehicle crash that killed 1 and injured 2 others.
Source: http://kron4.com/2016/01/16/one-person-dead-in-a-fatal-car-accident-on-highway-4-in-martinez/

9. *January 16, Schenectady Daily Gazette* – (New York) **CSX train derailed west of Schenectady.** Rail traffic was suspended for several hours January 16 after three cars from a CSX freight train headed to Willard, Ohio, derailed near Pattersonville, New York. Crews worked to get the cars back on the tracks and resume train services.
Source: http://www.dailygazette.com/news/2016/jan/16/dot-csx-train-derailed-schenectady/

10. *January 15, WKYT 27 Lexington* – (Kentucky) **Deadly crash closes highway in Anderson County.** Kentucky Highway 44 in Anderson County was closed for several hours January 15 following an accident that left one person dead and a second injured.
Source: http://www.wkyt.com/content/news/Deadly-crash-closes-highway-in-Anderson-County-365424001.html

Food and Agriculture Sector

11. *January 19, U.S. Food and Drug Administration* – (National) **Fresh Express announces precautionary recall of a limited quantity of 12 oz baby spinach due to possible allergen exposure.** Fresh Express Incorporated issued a voluntary precautionary recall January 15 for 350 cases of its Fresh Express Baby Spinach products packaged in 12-ounce bags after almond allergens were accidentally introduced into the production supply. The products were distributed to 15 States.
Source: http://www.fda.gov/Safety/Recalls/ucm482136.htm

12. *January 19, WSOC 9 Charlotte* – (North Carolina) **Perdue Chicken plant in Concord closed after pipe rupture.** The Purdue Chicken plant in Concord, North Carolina was shut down for repairs January 19 after a pipe supplying oil to an oven ruptured, causing the oil to vaporize and fill the plant with smoke January 18. More than three dozen firefighters responded to the scene and no injuries were reported.
Source: http://www.wsoctv.com/news/news/perdue-chicken-plant-concord-closed-after-pipe-rup/np7TX/

13. *January 18, Associated Press* – (Indiana) **Turkeys test positive for bird flu at nine Indiana farms.** Officials from the Indiana State Board of Animal Health announced January 16 that nine turkey farms in Dubois County were infected with a deadly strain of bird flu, prompting officials to declare quarantine zones on Dubois, Martin, Orange, Crawford, and Daviess counties.
Source: http://www.foxnews.com/health/2016/01/17/turkeys-test-positive-for-bird-flu-at-nine-indiana-farms.html

14. *January 18, Coshocton Tribune* – (Ohio) **Morning fire at Kraft extinguished; damage unknown.** Coshocton officials are investigating a January 18 fire at Kraft Foods plant in Coshocton County that prompted fire crews to remain on site for over 2 hours containing the incident. No injuries were reported.
Source: http://www.coshoctontribune.com/story/news/local/2016/01/18/morning-fire-kraft-extinguished-damage-unknown/78976254/

15. *January 17, U.S. Department of Agriculture* – (National) **Kayem Foods Inc. recalls chicken sausage products due to misbranding.** The Food Safety and Inspection Service announced January 16 that Massachusetts-based Kayem Foods Inc., recalled approximately 22,182 pounds of its Al Fresco Sweet Apple Chicken Sausage packaged in 12-ounce vacuum packed bags after the company received complaints that the product was misbranded with incorrect nutritional information and that the label did not

list pork as an ingredient. The products were shipped to retail locations nationwide.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-006-2016-release

16. *January 16, U.S. Food and Drug Administration* – (National) **Heritage International (USA) Inc, voluntarily recalls one lot of raw cashew pieces because of possible Salmonella health risk.** California-based Heritage International (USA) Inc. issued a voluntary recall January 15 for its Trader Joe's Raw Cashew Pieces product packaged in 16-ounce plastic bags after routine inspection revealed the presence of Salmonella in the products. The products were distributed to Trader Joe's stores in 31 States.
Source: http://www.fda.gov/Safety/Recalls/ucm482097.htm

17. *January 15, U.S. Food and Drug Administration* – (National) **Blendtech issues allergy alert on undeclared milk allergen in Uncle Buck's Fish Batter Mix - Original.** Kansas-based BlendTech Inc. issued a voluntary recall January 15 for its Uncle Buck's Fish Batter Mix – Original products packaged in 22-ounce bottles due to the presence of undeclared milk allergens. The products were distributed in Bass Pro Shops stores nationwide and through mail orders.
Source: http://www.fda.gov/Safety/Recalls/ucm482078.htm

Water and Wastewater Systems Sector

18. *January 18, WIFR 23 Freeport* – (Illinois) **City of Freeport issues boil order after water main break.** A citywide boil advisory was issued for Freeport, Illinois, January 18 – January 19 following a water main break at the city's water plant that spilled over 3 million gallons of water. Freeport School District cancelled classes as a precaution due to the advisory.
Source: http://www.wifr.com/home/headlines/City-of-Freeport-Issues-Boil-Order-365642001.html

19. *January 18, Associated Press* – (Florida) **Vandals drain 400K gallons from drinking water supply.** Authorities are investigating after vandals opened 20 water lines and drained approximately 400,000 gallons of drinking water in Flagler County, Florida, forcing officials to issue a precautionary boil water notice for approximately 1,700 people January 18.
Source:
http://www.gainesville.com/article/20160118/WIRE/160119643?Title=Vandals-drain-400K-gallons-from-drinking-water-supply

20. *January 17, San Antonio Post* – (Michigan) **White House declares emergency in Michigan over bad water.** The U.S. President declared a state of emergency in Michigan in response to lead-contaminated drinking water in the city of Flint, and authorized Federal aid for State and local response efforts in the county.
Source: http://www.sanantoniopost.com/index.php/sid/240343785

Healthcare and Public Health Sector

21. *January 16, U.S. Food and Drug Administration* – (California) **Abbott's Compounding Pharmacy issues voluntary recall of all lots of unexpired sterile human and animal compounded products due to lack of sterility assurance.** The U.S. Food and Drug Administration announced January 16 that Abbott's Compounding Pharmacy issued a voluntary recall for all unexpired lots of its sterile compounded injectable medications, sterile solutions, eye drops, and eye ointments distributed to patients, physician offices, clinics, and veterinarians in California due to concerns of a lack of sterility assurance following a Federal inspection.
Source: http://www.fda.gov/Safety/Recalls/ucm482101.htm

22. *January 14, Orange County Register* – (California) **Nearly 21,000 customer records hit by Blue Shield security breach.** Blue Shield of California announced January 14 that the personal information, including Social Security numbers, of nearly 21,000 individual and family plan customers was accessed in a security breach after a vendor who provides enrollment assistance was targeted by a phone scam at a call center in 2015. Customers who were impacted will be notified and offered free credit monitoring services.
Source: http://www.ocregister.com/articles/shield-699874-blue-security.html

Government Facilities Sector

23. *January 19, Boston Herald* – (Massachusetts) **Arlington high school evacuated after bomb threat.** Authorities are investigating after Arlington High School in Massachusetts was dismissed January 19 due to a phoned bomb and shooting threat made via robocall. Officials also investigated at least five hoax bomb threats called into State schools January 15.
Source:
http://www.bostonherald.com/news/local_coverage/2016/01/arlington_high_school_evacuated_after_bomb_threat

24. *January 15, Los Angeles Times* – (Utah) **Army says failures in leadership at biodefense lab led to mishandled anthrax shipments.** The U.S. Army announced findings from an internal investigation January 15 which determined that mismanagement and technical failures allowed the Army's Dugway Proving Ground biodefense facility in Utah to mistakenly send live anthrax samples to 194 commercial, academic, and Federal facilities from 2004 to 2015 via FedEx and other commercial shipping companies across all 50 states.
Source: http://www.latimes.com/nation/la-na-army-anthrax-20160115-story.html

For another story, see item **18**

Emergency Services Sector

25. *January 18, Brockton Enterprise* – (Massachusetts) **911 communications in Brockton restored after service interruption.** Residents were alerted after emergency 9-1-1

services in Brockton were down for more than 6 hours January 17 due to a car that crashed into a utility pole supporting the emergency line.
Source: http://www.wickedlocal.com/article/20160118/NEWS/160116516

26. *January 18, Prescott Daily Courier* – (Arizona) **Six hurt in juvenile detention center riot in Prescott.** The Yavapai County Superior Court announced that 3 inmates and 3 detention officers were injured in a January 17 riot at the Yavapai Juvenile Detention Center in Prescott that began when detainees assaulted officers. Police and sheriff's deputies responded and quelled the riot.
Source:
http://dcourier.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=154021

27. *January 16, WUSA 9 Washington, D.C.* – (Virginia) **All clear given for Va. police station after bomb threat.** The Arlington Police Station in Virginia was evacuated for more than 4 hours January 16 due to a hoax bomb threat.
Source: http://www.wusa9.com/story/news/local/virginia/2016/01/16/bomb-threat-reported-va-police-station/78917762/

Information Technology Sector

28. *January 19, Softpedia* – (International) **Yahoo fixes bug that could compromise email accounts when opening an email.** Yahoo! patched a cross-site scripting (XSS) vulnerability that affected its Mail's Web interface after a researcher from Finish found that the flaw allowed attackers to fully compromise email accounts by crafting an email with a malicious code in the message's body and sending the malicious email to a target. The vulnerability can be executed each time a user opens an email.
Source: http://news.softpedia.com/news/yahoo-fixes-bug-that-could-compromise-email-accounts-when-opening-an-email-499107.shtml

29. *January 19, SecurityWeek* – (International) **Siemens patches flaw in building automation products.** Siemens released firmware updates patching a reflected cross-site scripting (XSS) vulnerability for its automation products running on the OZW Web server after a researcher found the flaw affected login pages of the QZW672 and OZW772 embedded Web servers, which enabled attackers to redirect users to phishing Web sites, steal users' data, or convince users to download malware onto their devices.
Source: http://www.securityweek.com/siemens-patches-flaw-building-automation-products

30. *January 19, CSO Online* – (International) **Linux zero-day affects most Androids, millions of Linux PCs.** A security researcher from Perception Point discovered a new zero-day vulnerability affecting Android phones running 4.4 KitKat operating system (OS) and Linux machines running Kernel 3.8 or higher OS that can allow attackers to delete files, view private information, and install malicious programs on Android or Linux applications. Researchers reported that no exploits were observed in the wild.
Source: http://www.networkworld.com/article/3023447/security/linux-zero-day-affects-most-androids-millions-of-linux-pcs.html#tk.rss_all

31. *January 19, SecurityWeek* – (International) **Linux trojan takes screenshots every 30 seconds.** Security researchers from Doctor Web detected a new Linux trojan dubbed Linux.Ekoms.1 can help cybercriminals spy on users by searching through temporary folders for audio recordings and screenshots with the .aat, .sst, .ddt, and .kkt extensions in users' devices, which are uploaded to a remote server hardcoded within the malware. Once the stolen data is sent to the remote server, the data is encrypted and attackers can use the command and control (C&C) server to send various commands to the infected machine.
Source: http://www.securityweek.com/linux-trojan-takes-screenshots-every-30-seconds

32. *January 18, SecurityWeek* – (International) **Authentication flaw found in Advantech ICS Gateways.** Security researchers from Rapid7 discovered a serious authentication bypass vulnerability and a potential backdoor account in Advantech's EKI products that allowed attackers to bypass the authentication process by using any public key and password via the Dropbear SSH daemon, which was lacking a verification protocol. In addition, researchers discovered an alleged backdoor account after a hardcoded username and password could be used by an unauthenticated attacker to access a production device.
Source: http://www.securityweek.com/authentication-flaw-found-advantech-ics-gateways

33. *January 18, Softpedia* – (International) **Kaspersky warns of potential cyberattacks against World Economic Forum participants.** Kaspersky security experts reported that it is expecting advanced persistent threat (APT) groups to increase their efforts and attempts at hacking high-ranking officials' computers and mobile devices from various countries and companies at the World Economic Forum (WEF) in Davos, Switzerland. The security firm advised attendees to use Virtual Private Network (VPN) connections to browse the Internet, charge mobile devices from an outlet, and use passwords instead of PINs to protect devices.
Source: http://news.softpedia.com/news/kaspersky-warns-of-potential-cyberattacks-against-world-economic-forum-participants-499080.shtml

34. *January 18, The Register* – (International) **Updated Android malware steals voice two factor authentication.** A Symantec security researcher reported that the Android.Bankosy trojan malware can open a backdoor to activate unconditional call forwarding and silent mode on Android handsets, collect a list of system-specific information and send it to the command and control (C&C) server to register the infected device, and obtain a unique identifier to further communicate with the C&C server to receive commands.
Source:
http://www.theregister.co.uk/2016/01/18/updated_android_malware_steals_voice_two_factor_authentication/

35. *January 17, Softpedia* – (International) **DDoS attack hits Kickass Torrents, DNS servers crippled.** The largest Internet portal, Kickass Torrents reported that its Web site was offline for almost 24 hours after an unknown attacker conducted denial-of-

service (DDoS) attacks to its Web site's domain name servers (DNS), and that during the week of January 10, the Web site was hit with smaller DDoS attacks. Officials reported the Web site is running, but are anticipating further attacks.
Source: http://news.softpedia.com/news/ddos-attack-hits-kickass-torrents-dns-servers-crippled-499019.shtml

36. *January 15, SecurityWeek* – (International) **Apple's Gatekeeper bypassed again.** A security researcher from Synack discovered a Gatekeeper bypass technique that managed to bypass Apple's operating system (OS) X's Gatekeeper security feature by finding a signed application that loads and executes an external binary at runtime, create a .dmg file in which the external binary is replaced with a malicious file, and deliver the malicious file to users via injecting the file into insecure download connections or by uploading the file to third-party application stores. Apple released a temporary patch addressing the vulnerability.
Source: http://www.securityweek.com/apples-gatekeeper-bypassed-again

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

Communications Sector

Nothing to report

Commercial Facilities Sector

37. *January 18, Tacoma News Tribune* – (Washington) **3 injured, 20 displaced in Tacoma apartment complex fire.** A 2-alarm fire at the Woodmark apartments in Tacoma displaced 20 people, damaged 6 apartment units, and injured 3 people January 18. The cause of the fire is under investigation.
Source: http://www.thenewstribune.com/news/local/article55392765.html

38. *January 18, WBMA-LD 58 Birmingham* – (Alabama) **Firefighters battle church fire in Cullman County.** The Simcoe Worship Center in Cullman County sustained extensive damage January 18 after its youth facility caught fire following an alleged electrical error. The total amount of damages were unknown, but officials believe the facility was destroyed.
Source: http://abc3340.com/news/local/firefighters-battle-church-fire-in-cullman

Dams Sector

Nothing to report

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