Daily Open Source Infrastructure Report
11 August 2015

Top Stories

- The Alliance Pipeline from Canada to the U.S. was shut down August 7 for an indeterminate amount of time after hydrogen sulphide gas was found in the system. – *Canadian Press* (See item **1**)

- A St. George, Utah businessman and 4 others were charged August 7 in connection to a $300 million scheme in which the suspects allegedly used straw companies to charge customers' credit and debit cards. – *Deseret News* (See item **5**)

- The owner of Irvine, California-based Pacific Property Assets was convicted August 7 for his role in a Ponzi scheme in which his company cost investors and banks over $193 million. – *Orange County Register* (See item **7**)

- Delta Air Lines flight 1889 from Boston to Salt Lake City, Utah was diverted August 7 after hail and lightning cracked the plane's windshield, struck an engine housing, and damaged its weather and navigational equipment radome. – *CBS News* (See item **8**)

Fast Jump Menu

Energy Sector

1. *August 7, Canadian Press* – (International) **Pipeline shuts down a major natural gas line due to hydrogen sulphide gas in the system.** The Alliance Pipeline, which carries 1.6 billion cubic feet of natural gas daily from Canada to the U.S., was shut down August 7 for an indeterminate amount of time after hydrogen sulphide gas was found in the system.
Source: http://www.news1130.com/2015/08/07/pipeline-shuts-down-a-major-natural-gas-lines-due-to-hydrogen-sulphide-gas-in-the-system/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

2. *August 9, WKYT 27 Lexington* – (Kentucky) **Richmond firefighters investigating electrical fire at plating company.** Authorities are investigating an August 9 electrical fire at the Blue Grass Plating Company in Richmond, Kentucky, which started in a small tank with heaters and damaged part of the building, closing the plant until August 10.
Source: http://www.wkyt.com/home/headlines/-Richmond-firefighers-investigating-electrical-fire-at-plating-company-321215801.html

3. *August 7, U.S. Department of Labor* – (Ohio) **Republic Steel exposes workers repeatedly to fall, chemical and other hazards at Lorain, Ohio, steel mill.** The Occupational Safety and Health Administration cited Lorain-based Republic Steel August 7 with 3 repeated and 8 serious safety violations, including exposing workers to falls of about 20 feet, failing to mark lifting devices with rated weight capacity, and improperly labeling a hydrochloric acid dip tank for chemical hazards, among others. Proposed penalties total $162,400.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28488

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *August 7, Krebs on Security* – (California) **Tech firm Ubiquiti suffers $46M cyberheist.** Ubiquiti Networks Inc., reported in the week of August 3 that

cybercriminals stole $46.7 million from the company via a CEO fraud attack involving employee impersonation and fraudulent requests from an outside entity that targeted the company's finance department. The company discovered the fraud on June 5 and has been working to recover the funds.
Source: http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

5. *August 7, Deseret News* – (Utah) **St. George businessman, others charged in new Federal fraud indictment.** A St. George, Utah businessman and 4 others were charged August 7 in connection to a $300 million scheme in which the suspects allegedly set up a series of straw companies to charge customers' credit and debit cards after firms started to fine the now-defunct iWorks online marketing enterprise for excessive chargebacks to customers.
Source: http://www.deseretnews.com/article/865634093/Jeremy-Johnson-others-charged-in-new-federal-fraud-indictment.html?pg=all

6. *August 7, Reuters* – (California) **Zynga in $23 mln settlement over alleged fraud tied to IPO.** Zynga Inc., announced August 7 a settlement of $23 million to resolve allegations that the company defrauded shareholders about business prospects in the time surrounding its 2011 initial public offering by concealing declining user activity, failing to address upcoming changes in demand, and inflating its 2012 revenue forecast.
Source: http://www.reuters.com/article/2015/08/07/zynga-settlement-idUSL1N10I2NL20150807

7. *August 7, Orange County Register* – (California) **O.C. real estate executive found guilty on 11 counts in $170 million investor fraud.** The owner of Irvine-based Pacific Property Assets was convicted August 7 for his role in a Ponzi scheme in which his company cost investors and banks over $193 million by soliciting investments while misleading investors and lenders as the real estate firm continued to lose up to $2 million a month.
Source: http://www.ocregister.com/articles/estate-676565-stewart-real.html

Transportation Systems Sector

8. *August 10, CBS News* – (National) **Questions after Delta flight caught in damaging storm.** Delta Air Lines Flight 1889 from Boston to Salt Lake City, Utah was diverted to Denver International Airport after their Airbus A320 experienced severe turbulence, hail, and lightning, which cracked the aircraft's windshield, struck the engine, and damaged the radome that houses weather radar and navigational equipment. The U.S. Federal Aviation Administration is investigating the incident.
Source: http://www.cbsnews.com/news/delta-flight-hit-hail-lightning-storm-boston-salt-lake-city-lands-safely/

9. *August 9, NBC News* – (National) **Chicago-bound flight diverted after mid-air 10,000-foot drop.** United Express Flight 5919 from Charlotte, North Carolina to Chicago was diverted to Indianapolis International Airport after a pressurization issue caused a 10,000-foot vertical drop. No injuries were reported, and maintenance technicians are investigating the incident.

Source: http://www.nbcnews.com/news/us-news/chicago-bound-flight-diverted-after-mid-air-drop-n406671

10. *August 8, Santa Clarita Valley Signal* – (California) **Late night oil spill snarls traffic on Interstate 5.** A semi-truck spilled over 150 gallons of diesel fuel onto a portion of southbound Interstate 5 August 7, resulting in the closure of all lanes near Calgrove Boulevard. Two lanes were opened within an hour, and all lanes were open within three.
Source: http://www.signalscv.com/section/36/article/140861/

11. *August 8, Las Vegas Sun* – (Nevada) **Tractor spills about 75 gallons of diesel fuel on U.S. 95.** Northbound U.S. 95 at Railroad Pass in Nevada was shut down for approximately 4 hours August 7 after a tractor suffered mechanical issues and leaked 75 gallons of diesel fuel onto the road.
Source: http://lasvegassun.com/news/2015/aug/08/tractor-spills-about-75-gallons-diesel-fuel-us-95/

12. *August 7, Associated Press* – (Pennsylvania; Washington) **Seattle-bound flight makes emergency landing in Philadelphia.** American Airlines Flight 669 to Seattle made an emergency landing at Philadelphia International Airport August 7 after crews declared an emergency due to reports of flames coming from the plane's engine, which was later discovered to be the result of unburned fuel that burned off after takeoff. No injuries were reported, and passengers were placed on another Seattle-bound flight.
Source: http://www.king5.com/story/news/2015/08/07/seattle-flight-emergency-landing-philadelphia/31324561/

Food and Agriculture Sector

13. *August 9, Missouri Farmer Today* – (Missouri) **Diseased wheat plagues farmers.** The U.S. Food and Drug Administration restricted the concentration of wheat fields to one part per million for human food products August 9 after wheat fields tested positive for vomitoxin, also known as mycotoxin deoxynivalenol. The toxin can cause feed refusal and poor weight gain in some livestock.
Source: http://www.missourifarmertoday.com/news/crop/diseased-wheat-plagues-farmers/article_68431768-3af4-11e5-9764-4b2479373486.html

14. *August 8, U.S. Food and Drug Administration* – (Oregon; Washington) **Kent, Washington Firm issues allergy alert on undeclared peanut ingredients.** The U.S. Food and Drug Administration reported August 8 that Real Foods, a Seattle LLC of Kent, Washington, is recalling 29 cases of Harvest Slaw Kit and 13 cases of Broccoli Salad Kit due to an undeclared peanut allergen. The product was shipped to retail stores in Oregon and Washington.
Source: http://www.fda.gov/Safety/Recalls/ucm457673.htm

Water and Wastewater Systems Sector

15. *August 9, Farmington Daily Times* – (Colorado) **EPA says 3 million gallons of**

contaminated water released into Animas River. Officials from the U.S. Environmental Protection Agency reported August 9 that Gold King Mine discharged approximately 3 million gallons of contaminated water containing zinc, copper, iron, and other heavy metals into the Animas River after heavy machinery damaged a plug August 5. The polluted water is being contained and treated in 4 ponds at the site of the spill near Silverton, Colorado.
Source: http://www.daily-times.com/four_corners-news/ci_28611665/epa-now-says-3-million-gallons-contaminated-water

16. *August 8, KTBS 3 Shreveport* – (Texas) **Explosion at Texarkana water plant under control.** The Texarkana Water Utilities Water Treatment plant experienced an electrical outage after a motor pump malfunctioned and caused an explosion August 8. Authorities expect all operations to return to normal and the incident will not impact water customers.
Source: http://www.ktbs.com/story/29742226/explosion-at-texarkana-water-plant-under-control

Healthcare and Public Health Sector

17. *August 10, South Florida Business Journal* – (Florida) **Hialeah pharmacy owner pleads guilty to $1.6 million Medicare fraud.** The owner and operator of Miami-Dade County-based Biomax Pharmacy pleaded guilty August 7 to one count of health care fraud after submitting falsified Medicare claims from October 2012 – September 2013, resulting in approximately $1.58 million in misappropriated Medicare funds.
Source: http://www.bizjournals.com/southflorida/news/2015/08/07/hialeah-pharmacy-owner-pleads-guilty-to-fraud.html

Government Facilities Sector

18. *August 10, Associated Press* – (California) **Lake County's Jerusalem Fire explodes in size, could merge with nearby Rocky Fire.** The Jerusalem Fire reached 5,000 August 10 after it started August 9, prompting Lake County authorities to issue a mandatory evacuation order for residents of the rural Jerusalem Valley. Firefighters battling the nearby Rocky Fire, which has burned nearly 109 square miles, were reassigned to the Jerusalem Fire out of fears that the two could merge.
Source: http://www.news10.net/story/news/local/california/2015/08/10/lake-countys-jerusalem-fire-explodes-size-could-merge-nearby-rocky-fire/31401229/

19. *August 9, Las Vegas Review-Journal* – (Arizona) **Arizona brush fire grows, hundreds of homes evacuated.** Arizona's Bureau of Land Management announced August 9 the evacuation of 850 homes after the Willow Fire in Mohave Valley, Arizona, grew to approximately 6,000 acres.
Source: http://www.reviewjournal.com/news/nation-and-world/arizona-brush-fire-grows-hundreds-homes-evacuated

20. *August 8, Fresno Bee* – (California) **Two large fires rage in Sierra, Sequoia National Forests.** U.S. Forest Service firefighters battled the Rough Fire in the Sierra National

Forest August 8, which had reached 1,365 acres and threatened the Giant Sequoia National Monument. Firefighters were also working against the 5,364-acre Cabin Fire in Golden Trout Wilderness, California which was 83 percent contained as of August 8.
Source: http://www.fresnobee.com/news/local/article30495681.html

Emergency Services Sector

21. *August 7, Miami Herald* – (Florida) **Miami-Dade officer pleads guilty to fraud for role in credit-repair ring.** A Miami-Dade County police officer pleaded guilty to a conspiracy charge August 7 for participating in an alleged credit-repair ring by selling 159 fabricated identity theft police reports, which were then used to clear the credit histories of the purported victims.
Source: http://www.miamiherald.com/news/local/crime/article30455709.html

Information Technology Sector

22. *August 10, Softpedia* – (International) **First vulnerability found in Microsoft Edge, affects other software as well.** Security researchers discovered a vulnerability in Microsoft's Server Message Block (SMB) protocol used for local-network file-sharing impacting all versions of Windows, in which a faulty dynamic link library (DLL) could allow an attacker to extract user credentials from a closed Window domain via a man-in-the-middle (MitM) for SMB technique. The vulnerability affects Microsoft's new Edge Web browser, as well as various software from other developers.
Source: http://news.softpedia.com/news/first-vulnerability-found-in-microsoft-edge-affects-other-software-as-well-488913.shtml

23. *August 10, Securityweek* – (International) **HTC phone stores fingerprints in easily accessible plaintext.** Security researchers from FireEye discovered that several Android devices' fingerprint scanner authorization frameworks are vulnerable to exploitation, while others store fingerprints in plaintext and fail to secure the device's sensor.
Source: http://www.net-security.org/secworld.php?id=18742

24. *August 10, Securityweek* – (International) **Default WSUS configuration puts organizations at risk: researchers.** Security researchers from Context Information Security revealed that configuration issues in Microsoft Windows Update and Windows Server Update Services could be exploited in a situation in which secure sockets layer (SSL) communication is not enabled and a man-in-the-middle (MitM) attacker could modify metadata to create fake updates and execute arbitrary commands.
Source: http://www.securityweek.com/default-wsus-configuration-puts-organizations-risk-researchers

25. *August 9, IDG News Service* – (International) **Internal LTE/3G modems can be hacked to help malware survive OS reinstalls.** Security researchers from Intel reported that an unsecure Huawei LTE/3G modem firmware update process could allow an attacker to create a malicious firmware image that could be flashed by a malicious program to re-infect the main operating system (OS) even if it is reinstalled,

or could be modified to ignore future firmware updates.
Source: http://www.computerworld.com/article/2968274/security/internal-lte3g-modems-can-be-hacked-to-help-malware-survive-os-reinstalls.html#tk.rss_security

26. *August 9, IDG News Service* – (International) **SDN switches aren't hard to compromise, researcher says.** Security researchers from Hellfire Security revealed that software-defined network (SDN) switches running on the Open Network Install Environment (Onie) lacked authentication, encryption, access controls and permissions, potentially enabling an attacker to install persistent malware and monitor all network traffic running through a switch.
Source: http://www.computerworld.com/article/2959541/security/sdn-switches-arent-hard-to-compromise-researcher-says.html#tk.rss_security

27. *August 8, Securityweek* – (International) **Rush to put death records online lets anyone be 'killed'.** Security researchers at Def Con 2015 in Las Vegas revealed that flaws in online portals for submitting death and birth records could easily be exploited to create fake death and birth certificates due to a lack of authentication and credential protocols.
Source: http://www.securityweek.com/rush-put-death-records-online-lets-anyone-be-killed

28. *August 7, Securityweek* – (International) **Google disables inline installation of Chrome extensions for deceptive developers.** Google disabled inline installations for certain Chrome Web browser extension developers that the company has decided abused the feature to distribute the extensions via deceptive Web sites and advertisements, forcing redirects to extension product details on Chrome's Web store to provide users with information before installing.
Source: http://www.securityweek.com/google-disables-inline-installation-chrome-extensions-deceptive-developers

For another story, see item **4**

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

See item **23**

Commercial Facilities Sector

29. *August 10, WXIA 11 Atlanta* – (Georgia) **8 units damaged in Gwinnett apartment fire.** An August 10 fire at the Sinclair Apartments in Gwinnet County, Georgia,

displaced 20 people and damaged 8 units after the fire began on the second floor and spread to the roof of the building. The fire was contained and one resident suffered minor injuries.
Source: http://www.11alive.com/story/news/local/norcross/2015/08/10/gwinnett-apartment-fire/31398651/

30. *August 10, KWWL 7 Waterloo* – (Iowa) **14 departments battled bowling alley fire.** An August 9 fire severely destroyed the Donmar Lanes in Mt. Vernon, Iowa and prompted 140 firefighters from 14 different fire departments to respond. Fire crews contained the incident and the cause of the blaze remains unknown.
Source: http://www.kwwl.com/story/29746137/2015/08/09/fire-at-mt-vernon-bowling-alley

31. *August 10, WKMG 6 Orlando* – (Florida) **Orange County store evacuated for carbon monoxide, 7 hospitalized.** The Walmart Neighborhood Market in Orange County, Florida was evacuated August 9 for possible carbon monoxide poisoning that hospitalized 7 workers. Orange County Fire Rescue crews contained the incident.
Source: http://www.clickorlando.com/news/orange-county-store-evacuated-for-carbon-monoxide-7-hospitalized/34619470

32. *August 9, KSAT 12 San Antonio* – (Texas) **Two-alarm fire damages North Side apartments.** A 2-alarm fire damaged a San Antonio apartment complex August 9 after starting on the balcony of an apartment unit and damaging four apartment units. Damages total about $150,000.
Source: http://www.ksat.com/content/pns/ksat/news/2015/08/09/two-alarm-fire-damages-northside-apartments.html

33. *August 9, Palm Springs Desert Sun* – (California) **Indio apartment fire displaces 28.** Smoketree Apartments in Indio, California, sustained extensive damage August 9 after a roof fire displaced 28 residents. Damages total $1.5 million in losses.
Source: http://www.desertsun.com/story/news/local/indio/2015/08/09/crews-fighting-fire--indio-apartments/31366685/

Dams Sector

Nothing to report

<div style="border: 2px solid navy; padding: 20px;">

</div>