Daily Open Source Infrastructure Report
13 December 2016

Top Stories

- The president of Discovery Sales, Inc. pleaded guilty on behalf of his company December 8 to a builder bailout scheme that caused Wells Fargo & Company and JP Morgan Chase & Co. to suffer roughly $75 million in losses. – *San Jose Mercury News* (See item **4**)
- The former president of Culpeper, Virginia-based Capitol Components and Millwork, Inc. (CCM) pleaded guilty December 9 to a $10.5 million bank fraud scheme. – *U.S. Attorney's Office, Eastern District of Virginia* (See item **5**)
- An unlicensed physician who formerly worked at Detroit-based B&M Visiting Doctors PLC pleaded guilty December 8 to his role in a $6.3 million Medicare fraud scheme where he submitted falsified patient records to Medicare from 2005 – 2013. – *U.S. Department of Justice* (See item **17**)
- A 2-alarm fire at the Wood Lawn Garden Apartments in Alexandria, Virginia, displaced 67 residents and caused nearly $230,000 in damages December 10. – *WUSA 9 Washington, D.C.* (See item **25**)

Fast Jump Menu

Energy Sector

1. *December 10, Portland Oregonian; KATU 2 Portland* – (Oregon) **Ice wreaks havoc Saturday, but relents: 12,000 without power; Zoo Lights canceled.** Crews worked to restore power to roughly 12,000 customers across Portland, Oregon, who remained without power December 10 after winter storms snapped power lines and knocked out power to about 40,000 people. Authorities reported that around 100 people were stuck on a Metropolitan Area Express train for at least 3 hours December 9 after a power line fell on the tracks near Interstate 84 and Interstate 205.
   Source: http://www.oregonlive.com/portland/index.ssf/2016/12/post_570.html

2. *December 10, Berkeleyside.com* – (California) **Power outages affect large swaths of Berkeley.** Pacific Gas and Electric Company crews worked to restore power to 8,160 customers who remained without power December 10 following an outage that affected around 41,000 customers across Berkeley, Oakland, and Emeryville, California.
   Source: http://www.berkeleyside.com/2016/12/10/breaking-power-outages-affect-large-swathes-of-south-and-west-berkeley/

For another story, see item **9**

Chemical Industry Sector

See item **7**

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

3. *December 9, Brookfield-Elm Grove Now* – (Wisconsin) **Two charged for allegedly scamming credit unions for over $300K.** A Wisconsin couple was charged December 6 after the duo allegedly defrauded Enterprise Credit Union in Brookfield out of more than $300,000 after one of the defendants, who managed the bank's accounts, had her co-conspirator cash bank checks worth $980 several times each week beginning in May 2015. The charges allege that the couple used the money to buy drugs.
   Source: http://www.wauwatosanow.com/story/news/crime/2016/12/09/two-charged-allegedly-scamming-credit-unions-over-300k/95207718/

4. *December 9, San Jose Mercury News* – (California) **Homebuilder ordered to pay $11 million for "builder bailout" scam.** A northern California residential developer and president of Discovery Sales, Inc. pleaded guilty on behalf of his company December 8 to a builder bailout scheme where former Discovery Sales employees secured mortgages for buyers of more than 325 Seeno-built homes through illicit means and opened at least $1.24 billion in construction lines of credit, resulting in over $200 million in sales and roughly $75 million in losses to Wells Fargo & Company and JP Morgan Chase & Co. from 2006 – 2008. The executive agreed to pay $3 million in restitution to Fannie Mae and Freddie Mac as well as an $8 million fine, and the firm was placed on probation for 5 years.
Source: http://www.mercurynews.com/2016/12/08/homebuilder-albert-seeno-iii-ordered-to-pay-11-million-for-builder-bailout-scam/

5. *December 9, U.S. Attorney's Office, Eastern District of Virginia* – (Virginia) **Executive pleads guilty to $10.5 million bank fraud.** The former president of Culpeper, Virginia-based Capitol Components and Millwork, Inc. (CCM) pleaded guilty December 9 to a $10.5 million bank fraud scheme where the former executive fraudulently maintained a credit line at Fauquier Bankshares, Inc. by misrepresenting the company's true financial condition and submitting documents to the bank in October 2015 that fraudulently claimed there was roughly $17 million of total accounts receivable and inventory securing the bank's $11.5 million credit line, while in reality there was no more than $3.4 million of total accounts receivable and inventory. CCM was unable to repay the interest or principal amount of the loan.
Source: https://www.justice.gov/usao-edva/pr/executive-pleads-guilty-105-million-bank-fraud

Transportation Systems Sector

6. *December 12, WPTV 5 West Palm Beach* – (Florida) **Flight from Miami diverted to PBIA after possible fuel leak.** An American Airlines flight en route to Washington, D.C. from Miami International Airport was diverted to Palm Beach International Airport in Palm Beach County, Florida, December 11 after reports of a fuel leak. The plane landed safely and no injuries were reported.
Source: http://www.wptv.com/news/region-c-palm-beach-county/flight-from-miami-diverted-to-pbia-after-possible-fuel-leak

7. *December 11, Des Moines Register* – (Iowa) **Hazardous chemical spill shuts down I-80.** Westbound lanes of Interstate 80 near Anita, Iowa, were closed for several hours December 10 while crews worked to clean up a potentially explosive chemical after a semi-truck overturned and spilled an organic peroxide chemical on the roadway, which created a vapor cloud after mixing with snow. Eastbound Interstate 80 also experienced delays December 10 due to a fatal multi-vehicle crash that killed 3 people and injured 8 others.
Source: http://www.desmoinesregister.com/story/news/2016/12/11/hazardous-chemical-spill-shuts-down--80/95309024/

8. *December 10, WBBM 2 Chicago* – (Illinois) **Chicago area snowstorm leads to**

canceled flights at O'Hare, Midway. The Chicago Department of Aviation reported that over 1,200 flights at Chicago O'Hare International Airport and a total of 175 flights at Chicago Midway International Airport were canceled December 10 – December 11 due to a snowstorm.
Source: http://chicago.cbslocal.com/2016/12/10/chicago-area-snowstorm-leads-to-canceled-flights-at-ohare-midway/

9. *December 10, WTVH 5 Syracuse* – (New York) **I-690 in Baldwinsville reopens after tractor trailer rollover with an ethanol spill.** Interstate 690 in Baldwinsville, New York, was closed for nearly 9 hours December 10 after a semi-truck carrying 11,000 gallons of ethanol overturned and spilled its load on the roadway. The spill prompted authorities to issue a shelter-in-place order for 300 residents at the nearby Syracuse Home at McHarrie Place assisted living facility.
Source: http://cnycentral.com/news/local/tractor-trailer-rollover-shuts-down-690-in-baldwinsville

For another story, see item **1**

Food and Agriculture Sector

10. *December 12, Food Safety News* – (National) **Monkey bread mix recalled for Salmonella in powdered milk.** Brand Castle LLC issued a voluntary recall December 10 for approximately 168 cases of its "In the Mix" branded monkey bread mix products due to potential Salmonella contamination after the firm's ingredient supplier, Valley Milk Products LLC, recalled its buttermilk powder used in the monkey bread mix products due to Salmonella. No illnesses or adverse reactions have been reported and the products were shipped to a single retailer in 39 States.
Source: http://www.foodsafetynews.com/2016/12/monkey-bread-mix-recalled-for-salmonella-in-powdered-milk/#.WE6uRPkrKUk

11. *December 12, Food Safety News* – (National) **Chips recalled for Salmonella in powdered milk seasoning.** Shearer's Foods LLC issued a voluntary recall December 10 for 5 brands of its snack chips products due to potential Salmonella contamination after the firm was notified by a seasoning supplier that Valley Milk Products LLC recalled its nonfat high-heat milk powder and sweet buttermilk powder used in a variety of their seasonings due to Salmonella. No illnesses or adverse reactions have been reported.
Source: http://www.foodsafetynews.com/2016/12/135689/#.WE6q5vkrKUk

12. *December 12, U.S. Food and Drug Administration* – (National) **TreeHouse Foods announces voluntary product recall due to possible health risk.** TreeHouse Foods Inc. issued a recall December 11 for select macaroni and cheese cup products containing cheddar cheese seasoning due to potential Salmonella contamination after the firm received notification from its supplier that the milk powder used in the seasoning may be contaminated with Salmonella. No illnesses or adverse reactions have been reported and the products were distrusted to retailers nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm532762.htm

13. *December 11, U.S. Food and Drug Administration* – (National) **Boulder Brands, Inc. voluntarily recalls Earth Balance Vegan White Cheddar Mac & Cheese and Earth Balance Vegan Cheddar Mac & Cheese due to possible dairy allergen contamination.** Boulder Brands, Inc. issued a voluntary nationwide recall December 10 for its Earth Balance Vegan White Cheddar Mac & Cheese and Earth Balance Vegan Cheddar Mac & Cheese products after several consumers notified the company that the products may contain a dairy allergen.
Source: http://www.fda.gov/Safety/Recalls/ucm532675.htm

14. *December 9, U.S. Food and Drug Administration* – (National) **FAIRWAY "LIKE NO OTHER MARKET" recalls FAIRWAY brand Candy Corn because of possible health risk.** Fairway Market issued a voluntary recall December 8 for its FAIRWAY brand Candy Corn products due to the potential presence of undeclared eggs after the firm received a report of an allergic reaction. The products were distributed to Fairway stores in New York, New Jersey, and Connecticut, as well as via home delivery programs provided by Fairway E-commerce, Google, and Instacart.
Source: http://www.fda.gov/Safety/Recalls/ucm532380.htm

Water and Wastewater Systems Sector

15. *December 12, Bluefield Daily Telegraph* – (West Virginia) **'Water turned black, like coal': Gary residents waiting on test results after possible water contamination.** Gary, West Virginia officials issued an advisory December 9 warning the town's residents not to use water for drinking or cooking, even if it is boiled first, after water plant workers and residents noticed December 8 that the water turned black. Officials are testing water samples and the results are expected to be returned December 13.
Source: http://www.bdtonline.com/news/water-turned-black-like-coal-gary-residents-waiting-on-test/article_e7b5003e-c021-11e6-9d35-7faad160f45e.html

16. *December 11, Associated Press* – (Colorado; New Mexico; Utah) **EPA will pay $4.5M tied to '15 mine spill.** The U.S. Environmental Protection Agency (EPA) announced December 9 it will pay $4.5 million to State, local, and tribal governments for their emergency response to a 3 million-gallon wastewater spill at the inactive Gold King Mine in southwestern Colorado that the EPA inadvertently triggered during preliminary cleanup work in August 2015. The spill carried arsenic, lead, and other heavy metals into rivers, contaminated Colorado, New Mexico, and Utah waterways, and forced utilities, farmers, and ranchers to temporarily stop drawing water from the impacted rivers.
Source: http://www.nwaonline.com/news/2016/dec/11/epa-will-pay-4-5m-tied-to-15-mine-spill/?news

Healthcare and Public Health Sector

17. *December 9, U.S. Department of Justice* – (Michigan) **Unlicensed Michigan physician pleads guilty to conspiracy to commit wire fraud for role in $6.3 million Detroit-based Medicare fraud scheme.** An unlicensed physician who formerly worked at Detroit-based B&M Visiting Doctors PLC pleaded guilty December 8 to his role in a

$6.3 million Medicare fraud scheme where he falsified patient records, including medical documents, prescriptions for controlled substances, and billing documents, which he fraudulently submitted to Medicare from 2005 – 2013. Three co-conspirators previously pleaded guilty for their roles in the scheme.
Source: https://www.justice.gov/opa/pr/unlicensed-michigan-physician-pleads-guilty-conspiracy-commit-wire-fraud-role-63-million

For another story, see item **21**

Government Facilities Sector

18. *December 10, East Brunswick Patch* – (New Jersey) **South River schools evacuated Friday due to suspicious item.** Students at South River Elementary and Middle School in New Jersey were evacuated and ordered to shelter in place for several hours December 9 after a suspicious item was found outside the building. Police deemed the building safe after a search was conducted and no other suspicious items were found.
Source: http://patch.com/new-jersey/eastbrunswick/south-river-schools-evacuated-friday-due-suspicious-item

Emergency Services Sector

Nothing to report

Information Technology Sector

19. *December 12, Help Net Security* – (International) **New AirDroid releases fix major security issues.** The AirDroid team released mobile version 4.0.0.3 and Microsoft Windows and Apple Mac version 3.3.5.3 of its remote management tool for Android after Zimperium security researchers found the app does not verify if a served update is legitimate, and sends and receives information over insecure channels, thereby exposing users on unsecured networks to man-in-the-middle (MitM) attacks. In addition to the security improvements, the AirDroid developers also upgraded the communication channels to Hypertext Transfer Protocol Secure (HTTPS) and enhanced the encryption method.
Source: https://www.helpnetsecurity.com/2016/12/12/airdroid-fix-major-security-issues/

20. *December 12, SecurityWeek* – (International) **Dozens of teens arrested over DDoS attacks.** Europol announced that 34 arrests were made as part of a multi-national operation targeting users of distributed denial-of-service (DDoS) cyber-attack tools after the individuals allegedly paid for stressers and booters services to deploy malicious software to launch DDoS attacks. Authorities believe the tools used in the attacks are part of the illicit DDoS-for-hire services where a hacker can pay to have an attack carried out against a targeted victim.
Source: http://www.securityweek.com/dozens-teens-arrested-over-ddos-attacks

21. *December 12, SecurityWeek* – (International) **Samas ransomware gang made**

$450,000 in one year analysis. Palo Alto Networks researchers reported that the cybercriminals behind the Samas, or SamSa ransomware were carrying out targeted attacks against the healthcare industry and have collected over $450,000 in ransom payments from their targets since the beginning of 2016. The ransomware has undergone a series of modifications since it was first spotted, including changes to the encrypted filename extensions that are appended to files after encryption takes place in order to make analysis and reverse-engineering more difficult.
Source: http://www.securityweek.com/samas-ransomware-gang-made-450000-one-year-analysis

22. *December 12, Help Net Security* – (International) **New minimum code signing requirements for use by all CAs.** The Certificate Authority Security Council (CASC) announced that the Code Signing Working Group released new Minimum Requirements for Code Signing for use by all Certificate Authorities (CA) which represent the first standardized code signing guidelines and incorporate several new features to help businesses defend their systems from cyber-attacks, including stronger protection for private keys, certificate revocation, and improved code signatures time-stamping, among other features. Microsoft is the first applications software vendor to adopt the guidelines and will require CAs that issue code signing certificates for Windows platforms to adhere to the new requirements beginning February 1, 2017.
Source: https://www.helpnetsecurity.com/2016/12/12/code-signing-requirements/

23. *December 12, The Register* – (International) **Microsoft Edge's malware alerts can be faked, researchers say.** Security researchers discovered that malicious actors can abuse Microsoft's Edge Web browser to display legitimate-appearing malware warning messages by altering URL characters and appending a hash and a URL of a Website that appears to be authentic to forge a technical support scam page due to flaws in Edge's "ms-appx:" and "ms-appx-web:" protocols. The fraudulent warnings replace Edge's SmartScreen messages, which are displayed if the browser detects suspected malicious Websites, indicating that a nominated site displayed in the address bar is infected.
Source:
http://www.theregister.co.uk/2016/12/12/microsoft_edges_malware_alerts_can_be_faked/

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

24. *December 12, Help Net Security* – (International) **Critical flaw opens Netgear routers to hijacking.** Netgear is investigating after the Computer Emergency Response Team Coordination Center (CERT/CC) warned that several of the company's router models,

including R7000, R6400, and R8000, potentially among others, can be exploited by remote, unauthenticated attackers to execute Linux commands with root privileges on affected routers by appending the command to a URL and convincing a targeted victim to visit a maliciously crafted Website or a legitimate site that serves malicious ads. This access can be used to command a victim's router to attack other computers, for File Transfer Protocol, or to carry out any other malicious action the attacker wants.
Source: https://www.helpnetsecurity.com/2016/12/12/flaw-netgear-routers-hijacking/

Commercial Facilities Sector

25. *December 11, WUSA 9 Washington, D.C.* – (Virginia) **More than 67 without homes after Va. fire.** A 2-alarm fire at the Wood Lawn Garden Apartments in Alexandria, Virginia, displaced 67 residents and caused nearly $230,000 in damages December 10. Authorities believe the fire was caused by a mechanical failure of a natural gas furnace flue.
Source: http://www.wusa9.com/news/local/alexandria/more-than-40-without-homes-after-va-fire/367740760

26. *December 11, Kalamazoo Gazette* – (Michigan) **Almost half of Boyne Highlands lodge damaged by fire, resort closed indefinitely.** The Boyne Highlands Resort in Harbor Springs, Michigan, was closed until further notice after a fire damaged 40 percent of the main lodge and injured 12 people December 11. The cause of the fire remains under investigation.
Source: http://www.mlive.com/news/grand-rapids/index.ssf/2016/12/almost_half_of_boyne_highlands.html

27. *December 10, San Antonio Express-News* – (Texas) **Fire at downtown apartment complex forces evacuation.** Hundreds of people were evacuated following a fire at the Agave Apartments in San Antonio, Texas, December 10. No injuries were reported and the cause of the fire remains under investigation.
Source: http://www.mysanantonio.com/news/local/article/Crews-battling-fire-at-downtown-apartment-complex-10788423.php

For additional stories, see items **1** and **9**

Dams Sector

28. *December 11, WNEP 16 Scranton* – (Pennsylvania) **Flood wall worries in Wilkes-Barre.** Wilkes-Barre, Pennsylvania officials planned to meet December 12 to discuss a future course of action after a 40-foot section of the Solomon Creek flood wall fell into the water December 9. Crews put down tarps and sandbags to temporarily seal the damage, and the city's original plans to begin repairs of the flood wall the week of December 19 may change as a result of the break.
Source: http://wnep.com/2016/12/11/flood-wall-worries-in-wilkes-barre/

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