Daily Open Source Infrastructure Report
07 January 2016

Top Stories

- Utility crews began casting demister pads January 6 to contain an oily mist that appeared from a methane leak at the company's Aliso Canyon Storage Facility in California. – *Los Angeles Daily News* (See item **1**)
- Rapid7 discovered a flaw in the Comcast XFINITY Home Security system that can allow burglars to enter homes without triggering the alarm by causing interference or deauthentication to the ZigBee-based protocol. – *Help Net Security* (See item **4**)
- A former partner at McKinsey & Company's Chicago office and a former internal consultant for State Farm were charged January 5 for allegedly bilking both companies out of $900,000 in phony consulting fees. – *Chicago Sun-Times* (See item **6**)
- A Transit Express (TRAX) train was struck by a car in Salt Lake City January 4, killing 1 man, leaving 18 others injured, and causing the train to teeter on the North Temple overpass. – *KSL 5 Salt Lake City* (See item **10**)

Fast Jump Menu

Energy Sector

1. *January 6, Los Angeles Daily News* – (California) **Oily mist surfaces at Porter Ranch gas leak as well pressure drops.** Southern California Gas Company announced January 6 that crews began casting demister pads, which contain a mesh screen, to contain an oily mist that has appeared from a methane leak at the company's Aliso Canyon Storage Facility above Porter Ranch. The utility reported that the pads will trap droplets that mix with the gas as it rises.
   Source: http://www.dailynews.com/environment-and-nature/20160105/oily-mist-surfaces-at-porter-ranch-gas-leak-as-well-pressure-drops

2. *January 5, StateImpact Pennsylvania* – (Pennsylvania) **DEP fines Kinder Morgan for Philadelphia storage tank violations.** Kinder Morgan was issued a $745,000 fine by the Pennsylvania Department of Environmental Protection January 5 for violations at its Liquids Terminal in the Port Richmond section of Philadelphia, and for violations at its Point Breeze Terminal on Passyunk Avenue. The violations stem from an 8,000 gallon spill of fuel grade ethanol from an above ground storage tank at the Liquids Terminal and the accumulation of storm water in containment dykes at its Point Breeze Terminal.
   Source: https://stateimpact.npr.org/pennsylvania/2016/01/05/dep-fines-kinder-morgan-for-philadelphia-storage-tank-violations/

For another story, see item **3**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

3. *January 5, Kennewick Tri-City Herald* – (Washington) **Energy Northwest pays fine over Richland nuclear security.** Energy Northwest agreed to pay $35,000 to the U.S. Nuclear Regulatory Commission January 5 to settle allegations that the company had security issue incidences in which two security officers at the Columbia Generating Station in Washington were found to be inattentive at their posts. The company is required to install wide-angle cameras in bullet-resistant enclosures in towers to monitor the availability of nuclear security officers and revise its annual ethics and compliance training.
   Source: http://www.tri-cityherald.com/news/local/article53238340.html

Critical Manufacturing Sector

4. *January 6, Help Net Security* – (International) **Flaw in Comcast's home security system lets burglars in without triggering alarm.** A researcher at Rapid7 discovered a critical flaw in the Comcast XFINITY Home Security system that can allow burglars to enter homes without triggering the alarm by causing interference or deauthentication to the ZigBee-based communications protocol via commodity radio jamming

equipment and software-based deauthentication attacks on the protocol itself. There are currently no patches for the flaw.
Source: http://www.net-security.org/secworld.php?id=19288

Defense Industrial Base Sector

5. *January 6, CNN* – (International) **New Navy contract aims to equip hundreds of ships with drones.** The U.S. Department of Defense announced January 6 that a prototype for a "launch and recovery" system created to provide airborne surveillance and drone strikes from the decks of hundreds of U.S. Navy ships without deploying aircraft carriers or large, fixed land bases is scheduled for completion in November 2017.
Source: http://www.cnn.com/2016/01/06/politics/drones-aircraft-carriers-small-navy-ships/index.html

Financial Services Sector

6. *January 5, Chicago Sun-Times* – (National) **Former McKinsey partner, McLean County Board chair indicted for wire fraud.** A former partner at McKinsey & Company's Chicago office and a former internal consultant for State Farm were charged January 5 for allegedly bilking both companies out of $900,000 in phony consulting fees through two companies, Gabriel Solutions and Andy's BCB, while using the funds to pay for personal trips that were listed as business expenses.
Source: http://chicago.suntimes.com/news/7/71/1228078/former-mckinsey-partner-state-farm-consultant-facing-federal-wire-fraud-charges

Transportation Systems Sector

7. *January 6, Waterloo/Marshall Courier* – (Wisconsin) **Man killed in crash near Columbus.** Southbound lanes of State Highway 151 near Columbus were closed for more than 4 hours January 5 while officials investigated the scene of a fatal two-vehicle crash that killed one driver.
Source: http://www.hngnews.com/waterloo_marshall/news/local/article_7034bd3e-b487-11e5-b0d1-23339a52ab34.html

8. *January 5, Janesville Gazette* – (Wisconsin) **Driver in critical condition after car smashes into rear of school bus on Highway 14.** Highway 14 in Rock County was closed for more than 3 hours January 5 after a car rear ended a school bus, injuring three Evansville School District students and a driver.
Source:
http://www.gazettextra.com/20160105/driver_in_critical_condition_after_car_smashes_into_rear_of_school_bus_on_highway_14

9. *January 5, Fox News* – (Washington) **Spokane airport reopens after United jet skids into snowbank.** The Spokane International Airport in Washington was closed for approximately 2 hours January 5 after a United Airlines plane skidded off the taxiway and into a snowbank prior to takeoff. No injuries were reported.

Source: http://www.foxnews.com/us/2016/01/05/spokane-airport-closes-after-united-jet-skids-into-snowbank.html

10. *January 4, KSL 5 Salt Lake City* – (Utah) **Ogden man killed, 18 injured in TRAX train collision.** A Transit Express (TRAX) train was struck by a fast-moving car in Salt Lake City January 4, killing 1 man, leaving 18 others injured, and causing the train to teeter on the North Temple overpass after it was knocked off its tracks. Crews worked to remove the train and inspect the track.
Source: https://www.ksl.com/index.php?sid=38006765&nid=148&title=1-killed-trax-train-derailed-after-collision-on-north-temple&fm=home_page&s_cid=topstory

Food and Agriculture Sector

11. *January 5, U.S. Department of Agriculture* – (Louisiana) **Comeaux's Inc. recalls pork products due to possible Listeria contamination.** The Food Safety and Inspection Service announced January 5 that Louisiana-based Comeaux's Inc., issued a voluntary recall for 14 pounds of its Cajun Hickory Smoked Pork Tasso products sold in 1 pound vacuum-sealed packages due to possible Listeria monocytogenes contamination after the bacteria was discovered during routine testing. The products were sold in retail locations in Louisiana.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-002-2016-release

12. *January 5, U.S. Department of Agriculture* – (National) **Wegmans Food Markets recalls chicken products produced without the benefit of inspection.** The Food Safety and Inspection Service announced January 5 that Wegmans Food Markets Inc., announced a recall for approximately 1,125 pounds of its chicken products sold in 4 variations that were produced without the benefit of Federal inspection. The products were sold in Maryland, Massachusetts, Virginia, New Jersey, Pennsylvania, and New York.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-003-2016-release

Water and Wastewater Systems Sector

13. *January 5, Orange County Register* – (California) **Sewage spill closes section of ocean in Laguna Beach.** The Orange County Health Care Agency's environmental health division closed a 1,000-foot section of Laguna Beach from Calliope Street to Pearl Street January 5 due to a sewage spill that made its way into the ocean after it spilled from a manhole when a sewer line became clogged in the rain. The public was urged to stay out of the water for 72 hours following the rain.
Source: http://www.ocregister.com/articles/ocean-698684-health-officials.html

14. *January 5, Janesville Gazette* – (Wisconsin) **Janesville manhole overflows with 12,000 gallons of sewage; no threat to public safety.** Crews worked to clean up a 12,000 gallon sewage overflow in Janesville January 1 after a clogged pipeline blocked by grease caused the spill. Officials announced that the spill, which occurred over a

period of 2 hours, posed no threat to the environment or the public's health.
Source: http://www.gazettextra.com/20160105/janesville_manhole_overflows_with_12000_gallons_of_sewage_no_threat_to_public_safety

Healthcare and Public Health Sector

15. *January 5, WTNH 8 New Haven* – (Connecticut) **Trumbull dentist office evacuated after chemical spill.** Fire officials reported that Vaughn Family Dentistry in Trumbull was evacuated January 5 following a chemical spill of approximately 1 ounce of Formocresol, a disinfectant solution, in the office which caused 15 people to be treated on site and 6 others to be transferred to area hospitals.
Source: http://wtnh.com/2016/01/05/trumbull-dentist-office-evacuated-after-chemical-spill/

Government Facilities Sector

16. *January 6, Associated Press* – (Colorado) **Girl charged as adult in murder plot at Denver-area school.** Authorities announced January 6 that one of two juvenile females was charged while the second was arrested for allegedly conspiring to kill students and mapping out a plan for an attack at Mountain Vista High School in Castle Rock. Police were alerted of the plans December 12 via a text-a-tip program and continue to investigate.
Source: http://www.foxnews.com/us/2016/01/06/girl-charged-as-adult-in-murder-plot-at-denver-area-school.html

17. *January 5, WSAZ 3 Huntington* – (Ohio) **Students, driver injured in school bus rollover in Lawrence County, Ohio.** Ten students and the bus driver were transported to an area hospital after their school bus en route to South Point High School went off the road and landed on its side in a ditch on State Route 243 in Lawrence County, Ohio, January 5. The bus reportedly went off the road after a passing vehicle let off smoke and blocked the driver's view.
Source: http://www.wsaz.com/content/news/Several-injured-in-school-rollover-in-Lawrence-County-Ohio-364276501.html

18. *January 5, WFMJ 21 Youngstown* – (Ohio) **Seven Valley communities included in possible tax data breach.** The Regional Income Tax Agency of Ohio announced January 5 that as many as 50,000 people in the State may have had their personal information including Social Security numbers, compromised after a DVD was discovered missing in November which may have contained information from municipal tax documents dating on or before June 2012. The agency continues to investigate the incident.
Source: http://www.wfmj.com/story/30891154/seven-valley-communities-included-in-possible-tax-data-breach

19. *January 5, Boston Globe* – (Massachusetts) **Waltham elementary school evacuated due to carbon monoxide concerns.** Classes at Henry Whittemore Elementary School

in Waltham were cancelled January 5 due to an odor of natural gas and an unsafe level of carbon monoxide discovered by a maintenance worker prior to the start of the school day. Staff members were evacuated and crews worked to repair a malfunctioning boiler that prompted the odors.
Source: https://www.bostonglobe.com/metro/2016/01/05/waltham-elementary-school-staff-evacuated-due-carbon-monoxide-concerns/mg9qR4m5rs3egeqk1fqtDL/story.html

For another story, see item **8**

Emergency Services Sector

20. *January 6, Mohave Valley Daily News* – (Arizona) **City 911 service back to normal.** Emergency 9-1-1 service in Bullhead City was restored January 5 following a fiber connection failure January 3 from the main Frontier Communications Central Office to the Bullhead City Police Department which forced 9-1-1 calls to be rerouted through the Mohave County Sheriff's Office Dispatch Center until the issue was resolved.
Source: http://www.mohavedailynews.com/news/city-service-back-to-normal/article_fa484558-b447-11e5-9cc0-574cb1cd5fb4.html

21. *January 5, WLWT 5 Cincinnati* – (Kentucky) **2 prison escapees, including violent offender from NKY, caught in Harrison Co.** Authorities recaptured two inmates January 5 in Harrison County who escaped from the Blackburn Correctional Complex in Lexington January 4 following a tip from the public.
Source: http://www.wlwt.com/news/escapees-from-central-kentucky-prison-captured/37270140

Information Technology Sector

22. *January 6, SecurityWeek* – (International) **Linode resets user passwords after breach.** Linode reported that it reset customers' Linode Manager passwords after the company discovered that a massive distributed denial-of-service (DDoS) attack was launched on its Web site, data centers, and Domain Name System (DNS) infrastructure, in addition to multiple volumetric attacks that targeted its authoritative nameservers and public Web sites, which may have compromised user credentials' from the company's database. The exposed database included usernames, email addresses, password hashes, and encrypted two-factor authentication seeds.
Source: http://www.securityweek.com/linode-resets-user-passwords-after-breach

23. *January 6, SecurityWeek* – (International) **Researchers publish default passwords for ICS products.** SCADA StrangeLove research team released a list of default credentials for industrial control system (ICS) products from various vendors including industrial routers, programmable logic controllers (PLC), and wireless gateways, among other products, to reveal that default passwords can pose a serious vulnerability for systems if remotely accessed. The team reported that vendors should implement proper security controls such as establishing password strength policies and forcing users to change passwords on the first login.
Source: http://www.securityweek.com/researchers-publish-default-passwords-ics-

products

24. *January 6, SecurityWeek* – (International) **Vulnerability exposed Blackphone to complete takeover.** Silent Circle released updates for its privacy-focused Blackphone 1 mobile device that patched several security flaws including a modem vulnerability that can be exploited by attackers to take control of the device's functions through an open-access socket that interacts with an NVIDIA Icera modem binary named agps_daemon, embedded with elevated privileges, to communicate directly to the Blackphone modem and record anything it receives to the ttySHM3 port. Attackers disguised with shell user privileges could send commands to the modem to exploit the flaw.
Source: http://www.securityweek.com/vulnerability-exposed-blackphone-complete-takeover

25. *January 5, Softpedia* – (International) **Author of Linux.Encoder fails for the third time, ransomware is still decryptable.** Researchers from Bitdefender reported that a Linux.Encoder decryption tool was available for free following the discovery of a third version of the Linux.Encoder malware which has infected about 600 servers. The ransomware targets Web servers and looks to encrypt files used in Web hosting and Web development environments.
Source: http://news.softpedia.com/news/author-of-linux-encoder-fails-for-the-third-time-ransomware-is-still-decryptable-498483.shtml

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 items **23** and **24**

Commercial Facilities Sector

26. *January 6, NBC News* – (National) **FBI hunting woman in six jewelry store stickups across South.** FBI officials announced their search for a man and a woman January 6 after the two allegedly stole jewelry from a Jared Vault in North Carolina January 4. The pair has been linked to jewelry robberies at six stores in Florida, Georgia, South Carolina, and North Carolina since April.
Source: http://www.nbcnews.com/news/us-news/fbi-hunting-woman-six-jewelry-store-stickups-across-south-n490991

27. *January 5, WJHG 7 Panama City/WECP 18 Panama City* – (Florida) **Best Buy**

remains closed as crews assess damage from fire. Officials reported January 5 that a Best Buy store in Panama City will be closed indefinitely during an assessment of the total amount of damages following a January 4 fire that allegedly started from an electrical short in a printer.
Source: http://www.wjhg.com/home/headlines/Fire-smoke-damage-Best-Buy-in-Panama-City-364202541.html

28. *January 5, Old Town Alexandria Patch* – (Virginia) **Gym members collapse from dangerous carbon monoxide levels.** The XSport Fitness gym in Alexandria, Virginia, was evacuated and closed January 2 after emergency crews discovered high levels of carbon monoxide in the air following reports of people collapsing at the gym. At least five people went to area hospitals for treatment and officials reported that either a gas-fired swimming pool heater or a fan, designed to keep it ventilated, malfunctioned.
Source: http://patch.com/virginia/oldtownalexandria/gym-members-collapse-dangerous-carbon-monoxide-levels

29. *January 5, Orange County Register* – (California) **Stanton gas leak prompts evacuation of nearby businesses.** Crews stopped the flow of gas from an inadvertently punctured 3-inch gas line in Stanton about 3 hours after several businesses were evacuated, a condominium complex was told to shelter in place, and southbound lanes of Village Center Driver were closed January 5.
Source: http://www.ocregister.com/articles/gas-698632-nearby-businesses.html

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