Daily Open Source Infrastructure Report
07 November 2013

Top Stories

- California regulators fined Pacific Gas and Electric Co. $8.1 million for flawed pipe inspections of 224 welds on natural gas pipelines from Petaluma to Lodi. – *San Francisco Chronicle* (See item **1**)

- An Office of Inspector General and Office of Audits and Inspections audit revealed that 29 new weaknesses emerged from the U.S. Department of Energy's network in 2013, which do not include older flaws that were found but have not been addressed. – *Threatpost* (See item **29**)

- Researchers have detected a new variant of the Shiz remote access trojan (RAT) being used to search infected systems for SAP applications, potentially as the reconnaissance phase of an attack campaign. – *The Register* (See item **31**)

- A suspicious fire at Hampton Greens in Bellevue, Washington, destroyed 10 apartments, injured 7 people, and caused an estimated $1.5 million in damages. – *Seattle Times* (See item **43**)

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 5, San Francisco Chronicle* – (California) **PG&E fined $8 million for flawed pipe inspections.** Pacific Gas and Electric Co. (PG&E) was fined $8.1 million November 5 by California regulators for the contractor, TC Inspections Inc.'s, faulty inspections of 224 welds on natural gas pipelines from Petaluma to Lodi during a testing replacement program that the utility company began after a 2010 San Bruno explosion that killed eight people. PG&E is excavating and re-inspecting the lines. Source: http://www.sfgate.com/bayarea/article/PG-amp-E-fined-8-million-for-flawed-pipe-4958491.php

[Return to top]

Chemical Industry Sector

2. *November 5, Chicago Tribune* – (Illinois) **18 treated, 2 hospitalized after hazardous spill at SW chemical plant.** Fumes from a chemical spill of a heat transfer fluid at Stepan Chemical's Millsdale plant in southwest Elwood sickened 18 workers and led to a response by fire departments and emergency service personnel November 5. Source: http://www.chicagotribune.com/news/local/breaking/chi-hazardous-materials-spill-at-southwest-suburban-chemical-plant-20131105,0,6074686.story

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *November 6, Pittsburgh Tribune-Review* – (Pennsylvania) **Electrical fire shuts down reactor at Beaver County nuclear power plant.** A small electrical fire outside of an electrical generation turbine caused the operators of the Beaver Valley Power Station in Shippingport to shut down the Unit 1 reactor November 5. Source: http://triblive.com/news/adminpage/5012927-74/fire-plant-beaver

[Return to top]

Critical Manufacturing Sector

4. *November 5, New England Cable News* – (Massachusetts) **2 workers injured in explosion at Woburn, Mass. industrial park.** Two people were injured November 5 after an explosion at a Powderpart facility in an industrial park in Woburn. Authorities are investigating the cause of the explosion. Source: http://www.necn.com/11/05/13/2-workers-injured-in-explosion-at-Woburn/landing.html?blockID=856905&feedID=11106

[Return to top]

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *November 6, Eugene Register-Guard* – (Oregon) **'Tall Man' admits robberies.** A man known as the "Tall Man Bandit" pleaded guilty November 5 to robbing four banks in Eugene and two in Springfield during February and March.
Source: http://registerguard.com/rg/news/local/30693095-75/evans-bank-eugene-banks-march.html.csp

6. *November 5, Tulsa World* – (National) **Tulsa woman admits guilt in six-figure prepaid debit card fraud.** A Tulsa, Oklahoma woman pleaded guilty November 5 to her part in a multistate prepaid debit card fraud scheme that caused losses of between $200,000 and $400,000. The woman and her conspirators would induce employees at Walmart stores to activate prepaid debit cards by falsely claiming to be from the company's headquarters or from prepaid debit card company Green Dot.
Source: http://www.tulsaworld.com/news/crimewatch/tulsa-woman-admits-guilt-in-six-figure-prepaid-debit-card/article_7fdf9558-4673-11e3-bb78-0019bb30f31a.html

7. *November 5, Softpedia* – (International) **Cybercriminals use Android trojan Svpeng for mobile phishing.** Researchers at Kaspersky found that the Svpeng Android trojan has been enhanced with the ability to perform mobile phishing attacks targeting online banking and credit card information. The trojan currently targets Russian users but is already equipped with the ability to check for operating system language versions.
Source: http://news.softpedia.com/news/Cybercriminals-Use-Android-Trojan-Svpeng-for-Mobile-Phishing-397388.shtml

Transportation Systems Sector

8. *November 6, McClatchy Washington Bureau* – (National) **5 years after deadly crash, new pilot training rule becomes official.** The U.S. Federal Aviation Administration (FAA) on November 5 finalized a new rule that reauthorizes the FAA to take steps to prevent pilot fatigue and to address midair stalls, among other safety improvement issues. The rule originated from the crash of Colgan Air Flight 3407 near Buffalo, New York, in which the National Transportation Safety Board found that the flight crew members were not adequately trained.
Source: http://www.sacbee.com/2013/11/05/5884010/5-years-after-deadly-crash-new.html

9. *November 6, WJLA 7 Washington, D.C.* – (Virginia) **I-95 South fuel spill causes major traffic delays.** An accident involving a semi-truck that spilled more than 100

gallons of fuel on southbound Interstate 95 caused all lanes to be backed up for nearly 4 hours November 6.
Source: http://www.wjla.com/articles/2013/11/i-95-south-fuel-spill-causing-major-traffic-delays-96477.html

10. *November 5, Bristol Herald Courier* – (Tennessee) **Private aircraft on training exercises veers off runway at TCRA.** An accident involving a small plane that veered off a runway at Tri Cities Regional Airport in Blountville during a training exercise closed the runway for nearly 2 hours, impacting a number of flights November 5. The National Transportation Safety Board is investigating the incident.
Source: http://www.tricities.com/news/local/article_bc1b10ce-4650-11e3-865a-001a4bcf6878.html

11. *November 5, Associated Press* – (Texas) **NTSB faults parade plans in fatal Texas train collision.** Federal investigators on November 5 faulted a lack of safety planning by parade organizers and the city of Midland for a fatal crash November 15, 2012 involving a freight train that crashed into a semi-truck towing a parade float that killed 4 and injured 11 others.
Source: http://news.msn.com/us/ntsb-faults-parade-plans-in-fatal-texas-train-collision

12. *November 5, Fairbanks Daily News Miner* – (Alaska) **Alaska Highway reopened east of Tok.** An accident involving a semi-truck that caught fire on the Alaska Highway between Tok and Northway in Fairbanks closed the highway for about 7 hours November 5.
Source: http://www.newsminer.com/news/alaska_news/alaska-highway-reopened-east-of-tok/article_544c0646-4638-11e3-9752-001a4bcf6878.html

13. *November 5, WNEP 16 Scranton* – (Pennsylvania) **Gas leak shuts down busy highway near Selinsgrove.** A gas leak that occurred near Selinsgrove when contractors accidentally cut a gas line closed the four-lane highway on Routes 11 and 15 for several hours November 5.
Source: http://wnep.com/2013/11/05/gas-leak-shuts-down-busy-highway-near-selinsgrove/

14. *November 5, Malibu Times* – (California) **Three-Car crash leaves man with life-threatening injuries.** A three-vehicle accident involving two cars and a motorcycle on westbound Pacific Coast Highway and Busch Drive in California injured three people and closed westbound lanes for an undisclosed amount of time November 5. One person was arrested following the crash.
Source: http://www.malibutimes.com/news/article_a944a2ba-467a-11e3-99a5-0019bb2963f4.html

[Return to top]

Food and Agriculture Sector

15. *November 5, Chicago Sun-Times* – (Illinois) **Fire halts production at Blommer chocolate factory.** A fire at the Blommer Chocolate Company in West Town halted chocolate production, caused the evacuation of more than 100 workers from the facility, and closed West Kinzie Street between North Desplaines and North Clinton for more than an hour November 4. The fire is under investigation.
Source: http://chicago.cbslocal.com/2013/11/05/fire-halts-production-at-blommer-chocolate-factory/

16. *November 4, Associated Press* – (New Mexico; Missouri) **U.S. appeals court halts slaughter of horses for meat.** A U.S. Circuit Court of Appeals in Denver, Colorado, issued a temporary injunction November 4 halting the U.S. Department of Agriculture's inspections of horse slaughter plants in New Mexico and Missouri.
Source: http://www.cbsnews.com/8301-201_162-57610805/u.s-appeals-court-halts-slaughter-of-horses-for-meat/

17. *November 4, U.S. Food and Drug Administration* – (National) **Gourmet Express LLC. voluntarily recalls 32 ounce packages of "fusia chicken lo mein" and 21 ounce packages of "bremer 3 cheese chicken" and "bremer garlic shrimp" due to possible undeclared eggs.** Gourmet Express, LLC. voluntarily recalled fusia chicken lo mein, bremer 3 cheese chicken, and bremer garlic shrimp products due to possible undeclared eggs November 4. The recall was initiated after discovery that the egg-containing product was distributed in packaging that did not reveal the presence of eggs.
Source: http://www.fda.gov/Safety/Recalls/ucm373746.htm

[Return to top]

Water and Wastewater Systems Sector

18. *November 5, Pekin Daily Times* – (Illinois) **'Mount Gushmore' prompts water main replacement.** The Village of Tremont reported November 4 that a water main break near the town's water tower spilled between 250,000 and 300,000 gallons of water within 5-6 hours October 30. Officials decided to replace the main with a plastic one in order to avoid future erosion.
Source: http://www.pekintimes.com/article/20131105/NEWS/131109740/1001/NEWS

19. *November 5, U.S. Environmental Protection Agency* – (Michigan) **EPA and City of Ishpeming complete work in Deer Lake Area of Concern.** The U.S. Environmental Protection Agency and the City of Ishpeming announced the completion of an $8 million project to prevent the flow of mercury-contaminated water into Lake Superior from the contaminated Deer Lake Area of Concern.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/AA337F814B73894485257C1A005C49C6

[Return to top]

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

20. *November 6, WRAL 5 Raleigh* – (North Carolina) **With dam leak repaired, Balsam Lake refilled.** The U.S. Forest Service announced repairs to Balsam Lake dam in North Carolina were completed and the lake was filled with water after a board was repaired when officials noticed a leak in the dam.
Source: http://www.wral.com/with-dam-leak-repaired-balsam-lake-refilled/13079992/

21. *November 5, Elko Daily Free Press* – (Nevada) **Suspicious package at Adobe Middle School contained curtain hardware.** Adobe Middle School in Elko was evacuated and classes were dismissed November 5 after the school received a suspicious package in the mail. Police deemed the package safe after an inspection determined it contained supplies to install a curtain.
Source: http://elkodaily.com/news/situation-cleared-at-adobe-middle-school/article_e8d5a936-464a-11e3-92b9-001a4bcf887a.html

22. *November 5, Associated Press* – (Iowa) **4 students injured after Clinton school bus crash.** Four students were transported to an area hospital with injuries after a truck collided with a Clinton Community School District bus in Clinton, Iowa, November 5.
Source: http://www.kwwl.com/story/23885975/2013/11/05/4-students-injured-after-clinton-school-bus-crash

23. *November 5, Boston Globe* – (Massachusetts) **Mass. Bay Community College evacuates campuses after threat.** Officials are investigating after Massachusetts Bay Community College evacuated all three of its campuses and cancelled classes November 5 after two written bomb threats were found at the school's Wellesley and Framingham campuses. Police searched the campuses and gave an all clear once nothing suspicious was found.
Source: http://www.bostonglobe.com/metro/2013/11/05/mass-bay-community-college-evacuates-campuses-after-threat/W9JqoQKlj1RIPMvgSQn7kL/story.html

24. *November 5, Durham Herald-Sun* – (North Carolina) **Four injured after Orange County school bus hits another bus.** Four students were transported to an area hospital for minor injuries after one Orange County Schools' bus crashed into a Pathways Elementary School bus in Hillsborough, North Carolina, November 5.
Source: http://www.thetimesnews.com/news/region-state/four-injured-after-orange-county-school-bus-hits-another-bus-1.230411

25. *November 5, Chattanooga Chattanoogan* – (Tennessee) **Audit of Sequatchie County government finds numerous errors.** An audit by the Tennessee Comptroller's office determined that the Sequatchie County government needs to correct 17 accounting and record-keeping findings including allowing multiple employees to share computer

usernames and passwords, allowing employees to share from the same cash drawer, and a lack of segregation of duties.
Source: http://www.chattanoogan.com/2013/11/5/262814/Audit-Of-Sequatchie-County-Government.aspx

26. *November 5, Salisbury Post* – (North Carolina) **Health Department: Rowan school has shigellosis outbreak.** The Rowan County Health Department investigated a suspected outbreak of shigellosis at Koontz Elementary School in North Carolina after health officials in Cabarrus County reported 64 people had symptoms and 21 were confirmed with shigellosis.
Source: http://www.salisburypost.com/article/20131105/SP01/131109810/1023/health-department-rowan-school-has-shigellosis-outbreak

27. *November 5, Navy Times* – (International) **Sailors may have received botched flu vaccine.** U.S. Navy sailors aboard the USS Bonhomme Richard received another round of flu vaccine shots after an initial shipment of 1,380 flu shots were rendered potentially useless due to a shipping error. Officials determined the shots were sent alongside refrigerated cargo and the cold temperature may have compromised the vaccine's potency.
Source: http://www.navytimes.com/article/20131105/NEWS/311050024/Sailors-may-received-botched-flu-vaccine

28. *November 4, Associated Press* – (Florida) **Navy training jet crashes in Pensacola, Fla.** Officials are investigating after a U.S. Navy training jet crashed at Naval Air Station Pensacola, leaving the flight instructor and student pilot with injuries.
Source: http://news.msn.com/us/navy-training-jet-crashes-in-pensacola-fla

29. *November 4, Threatpost* – (National) **DOE audit reveals new weaknesses, and unpatched older flaws.** An audit undertaken by the Office of Inspector General and the Office of Audits and Inspections revealed that 29 new weaknesses emerged from the U.S. Department of Energy's network in 2013 in addition to 10 existing that the agency failed to fix after a 2012 audit.
Source: http://threatpost.com/doe-audit-reveals-new-weaknesses-and-unpatched-older-flaws

[Return to top]

Emergency Services Sector

30. *November 5, San Bernardino Sun* – (California) **Stolen cop car found, man arrested with history of stealing police cars.** Police recovered an unmarked police car November 1 that was stolen from the San Bernardino City Hall parking lot October 21 and took the suspect into custody after finding the vehicle in the suspect's apartment complex.
Source: http://www.sbsun.com/general-news/20131105/stolen-cop-car-found-man-arrested-with-history-of-stealing-police-cars

[Return to top]

Information Technology Sector

31. *November 6, The Register* – (International) **It's the Shiz: Mutant RAT spotted gnawing at SAP apps.** Researchers have detected a new variant of the Shiz remote access trojan (RAT) being used to search infected systems for SAP applications, potentially as the reconnaissance phase of an attack campaign. The new variant includes its usual remote access features, as well as SAP-related capabilities with an unknown purpose.
Source: http://www.theregister.co.uk/2013/11/06/sap_rat_malfeasance/

32. *November 6, Softpedia* – (International) **CSRF vulnerability in Twitter allowed hackers to read DMs, post tweets.** Twitter closed a cross-site request forgery (CSRF) vulnerability in its "add mobile device" feature after a researcher reported the issue. The vulnerability could have been leveraged to gain access to a user's direct messages and to post tweets.
Source: http://news.softpedia.com/news/CSRF-Vulnerability-in-Twitter-Allowed-Hackers-to-Read-DMs-Post-Tweets-397654.shtml

33. *November 6, Softpedia* – (International) **FBI adds 5 hackers to Cyber Most Wanted list.** The FBI added five new alleged cybercriminals to its Cyber Most Wanted list, including two accused of causing $50 million in damages by hacking into business telephone systems.
Source: http://news.softpedia.com/news/FBI-Adds-5-Hackers-to-Cyber-Most-Wanted-List-397572.shtml

34. *November 5, Krebs on Security* – (International) **Microsoft warns of zero-day attack on Office.** Microsoft warned users of a zero day vulnerability in some versions of Office on systems running older versions of Windows. Microsoft offered a fix-it tool until a comprehensive patch can be issued.
Source: http://krebsonsecurity.com/2013/11/microsoft-warns-of-zero-day-attack-on-office/

35. *November 5, Threatpost* – (International) **Marketplace for phony Twitter followers is big business.** Researchers at Barracuda Networks reported that cybercriminals behind fake Twitter accounts used to sell fake followers and spread malicious links have shifted to duplicating legitimate accounts in order to avoid detection and get better click-through rates on their malicious links.
Source: http://threatpost.com/marketplace-for-phony-twitter-followers-is-big-business

36. *November 5, IDG News Service* – (International) **Spike in traffic with TCP source port zero has some researchers worried.** Researchers at Cisco Systems reported a significant increase in TCP traffic with source port zero over the November 2-3 weekend. The increase in traffic could be a precursor to attempts to compromise networks.
Source:
http://www.computerworld.com/s/article/9243809/Spike_in_traffic_with_TCP_source_port_zero_has_some_researchers_worried

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: https://www.it-isac.org

[Return to top]

Communications Sector

37. *November 5, United Press International* – (Washington) **Copper thieves knock Spokane radio station off the air.** Radio station KMBI-AM in Spokane ceased broadcasting after copper thieves stole wire from the transmission tower November 3, disrupting transmission. The theft resulted in several thousand dollars in repairs needed to rewire the tower and return service.
Source: http://www.upi.com/Odd_News/2013/11/05/Copper-thieves-knock-Spokane-radio-station-off-the-air/UPI-31271383685851/

38. *November 5, Cincinnati Business Courier* – (National) **Kroger's wireless phone company faces $8.7M fine.** The Federal Communications Commission proposed fining I-Wireless $8.75 million in penalties for alleged abuse of the Lifeline program between October 2012 and April 2013.
Source: http://www.bizjournals.com/cincinnati/news/2013/11/05/krogers-wireless-company-faces-87m.html

39. *November 5, San Juan Islander* – (Washington) **Estimated 24 to 72 hours to repair broken fiber-optic line.** An underwater break in a fiberoptic line shut down CenturyLink-operated cellphone service, long distance land-line service, and 911 calls on Orcas, Shaw, and Lopez islands.
Source: http://sanjuanupdate.com/2013/11/internet-outage/

40. *November 5, Broadcasting & Cable* – (National) **FCC proposes fining TBS $25,000 over 'Conan' promo.** The Federal Communications Commission (FCC) proposed fining TBS $25,000 for a simulated Emergency Alert System warning used in a promotion that constituted a false distress signal in violation of FCC rules.
Source: http://www.broadcastingcable.com/article/496427-FCC_Proposes_Fining_TBS_25_000_Over_Conan_Promo.php

For another story, see item **7**

[Return to top]

Commercial Facilities Sector

41. *November 6, NJ.com* – (New Jersey) **3-alarm fire scorches Madison apartment**

building, fire chief says. A 3-alarm fire November 5 at the vacant Madison Manor Apartments in New Jersey caused severe damage to the top two floors of the building that was under renovation. Firefighters cleared the scene after 7 hours.
Source: http://www.nj.com/morris/index.ssf/2013/11/3-alarm_fire_scorches_madison_apartment_building_fire_chief_says.html

42. *November 6, WOAI 4 San Antonio* – (Texas) **300 people evacuated after hotel fire.** A fire that began in the main air conditioning unit at the Country Inn and Suites in San Antonio prompted the evacuation of 300 people from the hotel for 2 hours after smoke was sent through the building's ventilation system.
Source: http://www.news4sanantonio.com/news/features/top-stories/stories/300-hundred-people-evacuated-after-hotel-fire-5449.shtml

43. *November 5, Seattle Times* – (Washington) **7 injured as 10 apartments burn in suspicious Bellevue blaze.** A fire at Hampton Greens in Bellevue, Washington, November 5 destroyed 10 apartment units, left 7 people injured, and caused an estimated $1.5 million in damages to the building as well as $150,000 to the contents. Authorities are investigating the cause of the fire.
Source: http://seattletimes.com/html/latestnews/2022197529_bellevuefirexml.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

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.