



## Daily Open Source Infrastructure Report 07 December 2015

### Top Stories

- A December 3 explosion at the Ramsey Natural Gas Processing Plant near Orla prompted over 250 oil workers to evacuate, caused a 10-mile evacuation radius, and left 2 workers with injuries. – *Carlsbad Current-Argus* (See item [2](#))
- The U.S. Department of Justice unsealed a 92-count indictment December 3, charging numerous members of the International Federation of Association Football’s (FIFA) Executive Committee for their in role in a 24-year racketeering, wire fraud, and money laundering scheme. – *U.S. Department of Justice* (See item [7](#))
- Chipotle Mexican Grill, Inc. announced December 4 that it would overhaul its food-safety procedures and adapt all recommendations following a multi-State E. coli outbreak that sickened 45 people and forced restaurants closures in 2 States.– *USA Today* (See item [12](#))
- A carbon monoxide leak at Horace Mann Elementary School in Chicago caused 14 staff members and 139 students to be transported to area hospitals as a precaution December 3. – *Chicago Sun-Times* (See item [24](#))

---

### 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. *December 3, Raleigh News & Observer* – (North Carolina) **NC regulators find violations at another Duke coal ash deposit site.** The North Carolina Department of Environmental Quality cited Duke Energy and Charah Inc. December 2 for failing to notify the agency within 24 hours of a structural breach caused by severe erosion that exposed coal ash and a plastic cover to elements at its coal ash deposit site at the Asheville Regional Airport. The company responded that it took immediate steps to address the issue and install additional erosion and sediment controls at the site.  
Source: <http://www.newsobserver.com/news/business/article47755170.html>
2. *December 3, Carlsbad Current-Argus* – (Texas) **Workers escape serious injury after plant explosion.** A December 3 explosion at the Anadarko Petroleum Corporation-operated Ramsey Natural Gas Processing Plant near Orla, Texas, prompted over 250 oil workers to evacuate, caused a mandatory evacuation of people within a 10-mile radius, and left 2 workers with minor injuries. Operations at the plant were reduced and the cause of the explosion is under investigation.  
Source: <http://www.currentargus.com/story/news/local/new-mexico/2015/12/03/major-explosion-texas-gas-plant/76723494/>
3. *December 3, Los Angeles Times; Associated Press* – (West Virginia) **Executive convicted in West Virginia mine explosion that killed 29.** A Federal jury in West Virginia convicted the former Massey Energy chief executive December 3 for conspiring to willfully violate mine safety standards and for defrauding mine regulators following the 2010 coal mine explosion at West Virginia's Upper Big Branch mine that killed 29 men.  
Source: <http://www.latimes.com/nation/nationnow/la-na-nn-mine-explosion-trial-20151203-story.html>

For additional stories, see items [4](#) and [18](#)

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

4. *December 3, Los Angeles Times* – (California) **Regulators fine Edison \$16.7 million for secret San Onofre talks.** Southern California Edison was issued a \$16.7 million fine by the California Public Utilities December 3 for violating ex parte rules by failing to report that utility officials spoke with regulators over the closed San Onofre nuclear plant in California. Officials stated that the talks were related to the payment of costs surrounding the January 2012 shutdown of the nuclear plant.  
Source: <http://www.latimes.com/business/la-fi-regulators-fine-edison-20151203-story.html>

## Critical Manufacturing Sector

Nothing to report

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

5. *December 4, Southern California City News Service* – (California) **Ex-Beverly Hills broker charged in \$200 million stock scheme.** A Los Angeles man was taken into custody December 3 amid Federal charges that he and a German hedge fund manager defrauded investors of more than \$200 million from September 2004 to September 2007 by making illegal trades to boost the value of their co-owned company, Absolute Capital Management Holdings. The indictment also states that the suspect lied about \$10 million in illicit profits in a secret bank account on the Cook Islands.  
Source: <http://www.dailynews.com/general-news/20151203/ex-beverly-hills-broker-charged-in-200-million-stock-scheme>
6. *December 3, U.S. Department of Justice* – (Georgia) **Former bank teller pleads guilty to theft of public money.** A Columbus woman pleaded guilty in Federal court December 3 to one-count of theft of public money while she worked at a Suntrust Bank branch from February 2013 to May 2014 in which she cashed approximately 361 fraudulent tax returns to the U.S. Internal Revenue Service worth \$780,760.17 for numerous people in exchange for a fee.  
Source: <http://www.justice.gov/opa/pr/former-bank-teller-pleads-guilty-theft-public-money>
7. *December 3, U.S. Department of Justice* – (International) **Sixteen additional FIFA officials indicted for racketeering conspiracy and corruption.** Officials from the U.S. Department of Justice unsealed a 92-count indictment December 3 that charged numerous high-ranking members of the International Federation of Association Football's (FIFA) Executive Committee, Confederation of North, Central American, and Caribbean Association of Football (CONCACAF), and other suspects with ties to global soccer organizations for their role in a 24-year racketeering, wire fraud, and money laundering scheme in which soccer officials accepted over \$200 million in bribes to sell lucrative media rights for tournaments and matches.  
Source: <http://www.justice.gov/opa/pr/sixteen-additional-fifa-officials-indicted-racketeering-conspiracy-and-corruption>

## Transportation Systems Sector

8. *December 4, Associated Press* – (Tennessee) **CSX paid local agencies more than \$430K for train derailment.** CSX Transportation paid over \$431,000 to local agencies in Blount County and the cities of Maryville and Alcoa December 4 as reimbursement to officials who responded to the July 1 evacuation and cleanup that lasted 2 day after a

- train carrying hazardous material derailed and caught fire in eastern Tennessee.  
Source: <http://www.local8now.com/news/headlines/CSX-paid-local-agencies-more-than-430K-for-train-derailment-360541301.html>
9. *December 4, KETR 88.9 FM Commerce* – (Texas) **State Highway 24 remains closed due to flooding.** Texas State Highway 24 between Cooper and Commerce remained closed December 4 due to flooding following storms and the cresting of Cooper Lake December 1. Officials are working to release the excess water.  
Source: <http://ketr.org/post/state-highway-24-remains-closed-due-flooding>
  10. *December 4, KGW 8 Portland* – (Oregon) **1 dead, at least 8 hurt in crash near Lebanon.** Highway 34 in Lebanon, Oregon, was closed for approximately 5 hours December 3 following a 3-vehicle accident that left 1 person dead and at least 8 others injured.  
Source: <http://www.kgw.com/story/news/local/2015/12/03/8-injured-1-dead-after-crash-near-lebanon-police-say/76760476/>
  11. *December 3, East Oregonian* – (Oregon) **Fatal crash closes Highway 395.** Highway 395 in Oregon was closed for several hours December 3 while officials investigated the scene of a fatal 2-vehicle crash involving a semi-truck and a car that killed 1 driver.  
Source: <http://www.eastoregonian.com/eo/local-news/20151203/fatal-crash-closes-highway-395>

## **Food and Agriculture Sector**

12. *December 4, USA Today* – (National) **Chipotle overhauls safety standards after E. coli outbreak.** Chipotle Mexican Grill, Inc. officials announced December 4 that it would overhaul its food-safety procedures and adapt all recommendations sent by Seattle-based IEH Laboratories following a multi-State E. coli outbreak that sickened 45 people and forced restaurants in Oregon and Washington to close November 20.  
Source: <http://www.usatoday.com/story/money/2015/12/04/chipotle-commits-new-standards-after-ecoli-outbreak/76774132/>
13. *December 4, U.S. Food and Drug Administration* – (National) **Lipo Escultura Corp. issues nationwide recall of Lipo Escultura due to undeclared sibutramine and diclofenac.** Brooklyn-based Lipo Escultura Corp. dba JAT Productos Naturales Corp., and JAT Natural Products Corp. issued a voluntary recall of all Lipo Escultura weight loss dietary supplement products December 3 after U.S. Food and Drug Administration testing found the presence of undeclared and harmful sibutramine and diclofenac. Products were sold nationwide via Internet sales and in retail stores in New York.  
Source: <http://www.fda.gov/Safety/Recalls/ucm475550.htm>
14. *December 4, WLWT 5 Cincinnati* – (Kentucky) **Explosion, fire at Erlanger candy factory.** Hundreds of employees were evacuated from the Parfetti Van Melle candy factory located in Erlanger December 4 after a 3-alarm fire and explosion caused the factory to close and production to cease for the remainder of the day. Officials are investigating the cause of the fire.

Source: <http://www.wlwt.com/news/explosion-and-fire-at-erlanger-candy-factory/36792232>

15. *December 4, U.S. Environmental Protection Agency* – (National) **J.R. Simplot Company to reduce emissions at sulfuric acid plants in three states.** J.R. Simplot Company agreed to pay \$43 million to the U.S. Environmental Protection Agency and the U.S. Department of Justice December 3 to resolve allegations that the company violated the Clean Air Act law after modifying 5 of its sulfuric acid plants in 3 States. Simplot will implement a plan to monitor sulfur dioxide (SO<sub>2</sub>) emissions and install, update, and operate pollution controls that will decrease sulfur dioxide emissions SO<sub>2</sub> at the plants.  
Source: <http://yosemite.epa.gov/opa/admpress.nsf/0/18443BC3853924A685257F1000635BFE>
16. *December 3, U.S. Department of Agriculture* – (International) **K. Heeps recalls pureed meat products due to misbranding and undeclared allergens.** Allentown, Pennsylvania-based K. Heeps Inc. issued a recall December 3 for approximately 152,010 pounds of roast beef products after an in-plant inspection by the U.S. Department of Agriculture found that a vegetable flavoring in the product may contain undeclared milk and wheat allergens. Products were sent to distributors in Pennsylvania and Canada for institutional use.  
Source: [http://www.fsis.usda.gov/wps/portal/fsis/home!/ut/p/a0/04\\_Sj9CPYkssy0xPLMnMz0vMAfGjzOINAg3MDC2dDbwsfDxdDDz9AtyMgnyMDf3dDPQLsh0VAcy6FX0!/?1dmy&page=gov.usda.fsis.internet.newsroom&urile=wcm%3Apath%3A%2FFSIS-Content%2Finternet%2Fmain%2Ftopics%2Frecalls-and-public-health-alerts%2Frecall-case-archive%2Farchive%2F2015%2Frecall-145-2015-release](http://www.fsis.usda.gov/wps/portal/fsis/home!/ut/p/a0/04_Sj9CPYkssy0xPLMnMz0vMAfGjzOINAg3MDC2dDbwsfDxdDDz9AtyMgnyMDf3dDPQLsh0VAcy6FX0!/?1dmy&page=gov.usda.fsis.internet.newsroom&urile=wcm%3Apath%3A%2FFSIS-Content%2Finternet%2Fmain%2Ftopics%2Frecalls-and-public-health-alerts%2Frecall-case-archive%2Farchive%2F2015%2Frecall-145-2015-release)

## Water and Wastewater Systems Sector

17. *December 3, ColumbusUnderground.com* – (Ohio) **Columbus water management plan gains EPA approval.** The Ohio Environmental Protection Agency approved the Blueprint Columbus plan December 3 for the city of Columbus. The program will update aging infrastructure and create new water systems to help with storm water and wastewater management, and is expected to be carried out in phases over the next 20 years.  
Source: <http://www.columbusunderground.com/columbus-water-management-plan-gains-epa-approval>
18. *December 3, Associated Press* – (Alaska) **Fuel spills from tank supplying rural water treatment plant.** Crews worked December 3 to build a dike to prevent 2,000 gallons of diesel fuel that spilled from an overflowing fuel tank at the water treatment plant in Kiana from flowing downhill. The spill was discovered December 1 and the cause of the overflow remains under investigation.  
Source: <http://www.wral.com/fuel-spills-from-tank-supplying-rural-water-treatment-plant/15152744/>

## Healthcare and Public Health Sector

19. *December 3, Fort Collins Coloradoan* – (Colorado) **UCHealth nurse fired for viewing 800 patient records.** The University of Colorado Health announced December 3 that it notified 800 patients after a former Poudre Valley Hospital employee accessed their personal and medical information without authorization. The hospital fired the employee and will provide additional training to workers.  
Source: <http://www.coloradoan.com/story/news/2015/12/03/uchealth-nurse-fired-viewing-800-patient-records/76728016/>
20. *December 3, Santa Barbara Independent* – (California) **Cottage reports another records breach.** California-based Cottage Health reported December 3 that a breach in its server caused Google and Bing to index a limited amount of personal health information on as many as 11,000 patients from the hospital's 3 main campuses. The health system requested the removal of the information and continues to investigate the breach.  
Source: <http://www.independent.com/news/2015/dec/03/cottage-reports-another-records-breach/>

## Government Facilities Sector

21. *December 4, WIBW 13 Topeka* – (Kansas) **Onaga USD 322 cancels school after gas leak.** Onaga USD 322 in Kansas announced the cancellation of classes December 3 due to a lack of heat caused by a gas leak and regulator malfunction.  
Source: <http://www.wibw.com/home/headlines/Onaga-USD-322-cancels-school-after-gas-leak-360566311.html>
22. *December 3, Albuquerque Journal* – (New Mexico) **Computer trouble interferes with Bernalillo County jail, other operations.** Crews worked to restore service to the Bernalillo County government's computer systems December 3 following an outage that knocked out the county's Web site and email system. The outage disrupted some operations and held up the release of jail inmates.  
Source: <http://www.abqjournal.com/685371/news/abq-news/computer-trouble-interferes-with-bernalillo-county-jail-other-operations.html>
23. *December 3, KRTV 3 Great Falls/KXLH 9 Helena* – (Montana) **Overnight fire triggers evacuation at University of Great Falls dormitory.** Students from Providence Hall at the University of Great Falls in Montana were evacuated and relocated December 3 due to a small fire that began in a second floor bathroom. Students will be able to return to the dormitory once officials complete smoke removal and evaluate the total amount of damage.  
Source: <http://www.krtv.com/story/30660972/overnight-fire-triggers-evacuation-at-university-of-great-falls-dormitory>
24. *December 3, Chicago Sun-Times* – (Illinois) **More than 100 hospitalized after CO incident at South Side school.** A carbon monoxide leak December 3 at Horace Mann Elementary School in Chicago caused 14 staff members and 139 students to be

transported to area hospitals as a precaution. The school was evacuated and classes will be held in an annex building until the school building is deemed safe for re-entry.

Source: <http://chicago.suntimes.com/news/7/71/1149755/south-side-elementary-school-evacuated-high-co-levels>

## **Emergency Services Sector**

See item [22](#)

## **Information Technology Sector**

25. *December 3, Securityweek* – (International) **Ponmocup botnet still actively used for financial gain.** Researchers from Fox-IT released a report stating that the malware Ponmocup botnet has infected more than 15 million devices since 2009 and that its infrastructure consists of different components used to deliver, install, execute, and control the malware to prevent researchers from reengineering it. The botnet infects a device via encryption and stores its components in different locations to evade detection, while using different domains for installation, stealing file transfer protocol (FTP) and Facebook credentials to allow hackers to spread the malware.  
Source: <http://www.securityweek.com/ponmocup-botnet-still-actively-used-financial-gain>
26. *December 3, Securityweek* – (International) **Heartbleed, other flaws found in Advantech ICS Gateways.** Researchers from Rapid7 discovered that the newest firmware versions for Advantech Modbus gateway products including EKI-136X, EKI-132X, and EKI-122X were susceptible to Heartbleed attacks and Shellshock attacks which can be exploited via the Boa web server by administering any of the shell scripts in /www/sgi-bin. The vulnerabilities were tested with the genuine binaries in an emulator environment with a Metasploit module.  
Source: <http://www.securityweek.com/heartbleed-other-flaws-found-advantech-ics-gateways>
27. *December 3, Securityweek* – (International) **OpenSSL patches moderate severity vulnerabilities.** OpenSSL Project released updates to its cryptographic software library versions 1.0.2e, 1.0.1q, 1.0.0t, and 0.9zh, patching 3 vulnerabilities including the CVE-2015-3193 flaw that can produce incorrect results on x86\_64 systems via exploitation against RSA algorithms, Digital Signature Algorithms (DSA), and Diffie-Hellman (DH) algorithms; the CVE-2015-3194 flaw that can administer denial-of-service (DoS) attacks; and the CVE-2015-3195 flaw that can leak system memory when presented with a malformed X509\_ATTRIBUTE structure.  
Source: <http://www.securityweek.com/openssl-patches-moderate-severity-vulnerabilities>
28. *December 3, Softpedia* – (International) **Linux users targeted by new Rekoobe trojan.** Security researchers from Dr. Web reported that an updated version of the trojan, Linux.Rekoobe.1 can target Linux personal computers (PCs) running on Intel chips in 32-bit and 64-bit architectures by using the XOR algorithm to stop researchers

from detecting the trojan. The malware includes the functionality to download files from its command-and-control (C&C) server, upload files to the C&C server, and execute commands on the local shell, allowing attackers to deliver powerful payloads on infected systems.

Source: <http://news.softpedia.com/news/linux-users-targeted-by-new-rekoobe-trojan-497085.shtml>

For another story, see item [29](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto: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

29. *December 3, Securityweek* – (National) **Popular mobile modems plagued by zero-day flaws.** Security researchers with Positive Technologies tested mobile broadband modems and routers from Huawei, Gemtek, Quanta, and ZTE and found that the 3G/4G devices were vulnerable to remote code execution, had cross-site scripting (XSS) vulnerabilities, and lacked cross-site request forgery (CSRF) protection, among other issues, leaving the devices open to attackers for exploitation. Huawei was the only vendor that released firmware updates addressing the vulnerabilities, out of the four companies tested.

Source: <http://www.securityweek.com/popular-mobile-modems-plagued-zero-day-flaws>

## Commercial Facilities Sector

30. *December 3, Washington Post* – (Virginia) **Manassas Mosque gets threatening phone call: ‘You all will be killed.’** Prince William County police are investigating a threatening voicemail left December 3 at the Manassas Mosque in Virginia after the caller threatened to kill members of the mosque in retaliation to a fatal shooting in San Bernardino that killed 14 people and injured 21 others December 2.

Source: [https://www.washingtonpost.com/local/public-safety/manassas-mosque-gets-threatening-phone-call-you-all-will-be-killed/2015/12/03/494142b2-9a09-11e5-94f0-9eeaff906ef3\\_story.html](https://www.washingtonpost.com/local/public-safety/manassas-mosque-gets-threatening-phone-call-you-all-will-be-killed/2015/12/03/494142b2-9a09-11e5-94f0-9eeaff906ef3_story.html)

## Dams Sector

31. *December 3, WCIV 36 Charleston* – (South Carolina) **Army Corps dredges Breach Inlet, Jeremy Creek to fix problems.** The U.S. Army Corps of Engineers dredged 2 problem areas along the Atlantic Intracoastal Waterway in Mount Pleasant December 3, removing excess sand from the Breach inlet between Sullivan’s Island, the Isle of Palms, and Jeremy Creek in McClellanville. Officials estimated that the dredging

project will continue through 2016 and cost \$2.6 million

Source: <http://www.abcnews4.com/story/30663484/army-corps-dredges-breach-inlet-jeremy-creek-to-fix-problems>



**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 <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.