



## Daily Open Source Infrastructure Report 11 August 2016

### Top Stories

- Pacific Gas & Electric Co. was found guilty August 9 of violating pipeline safety regulations and failing to identify a high risk gas line prior to a fatal pipeline explosion in San Bruno, California, in 2010 that killed eight people. – *Associated Press* (See item [1](#))
- The former owner and operator of California-based Rodis Law Group pleaded guilty August 9 for his role in a \$9 million fraudulent mortgage modification scheme where he and others convinced over 1,500 homeowners to pay for fraudulent services from October 2008 – June 2009. – *Orange County Register* (See item [4](#))
- The U.S. Environmental Protection Agency fined the State of Hawaii Department of Land and Natural Resources August 8 for violating a Federal ban on large capacity cesspools on Maui and the Big Island. – *U.S. Environmental Protection Agency* (See item [14](#))
- Eight Florida residents were charged August 9 for their roles in a health care fraud scheme where the group allegedly submitted nearly \$663 million in fraudulent reimbursement claims from October 2012 – December 2015. – *U.S. Department of Justice* (See item [15](#))

---

### 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. *August 10, Associated Press* – (California) **Pacific Gas & Electric guilty: Utility convicted of obstruction in San Bruno blast probe.** Pacific Gas & Electric Co. (PG&E) was found guilty August 9 of violating pipeline safety regulations and misleading investigators about how the utility identified high-risk pipelines after the utility failed to gather information pertinent to evaluating potential gas line threats and failed to classify a gas line as high risk prior to a fatal natural gas pipeline explosion in 2010 that killed 8 people and destroyed 38 homes in San Bruno, California. The utility could be fined up to \$3 million for the violations.

Source: <http://www.smdailyjournal.com/articles/news/2016-08-10/pacific-gas-electric-guilty-utility-convicted-of-obstruction-in-san-bruno-blast-probe/1776425166449.html>

## Chemical Industry Sector

2. *August 8, WDAM 7 Laurel* – (Mississippi) **Hattiesburg's settlement amount with Hercules revealed.** A settlement between the City of Hattiesburg in Mississippi and Ashland, Inc., formerly known as Hercules, Inc., was released August 8 stating that the chemical company must pay the city \$3 million to resolve a 2013 lawsuit alleging that the Hercules plant knowingly and improperly disposed of hazardous waste, causing damage to the city's wastewater system.

Source: <http://www.wdam.com/story/32713200/hattiesburgs-settlement-amount-with-hercules-revealed>

## Nuclear Reactors, Materials, and Waste Sector

3. *August 9, Kennewick Tri-City Herald* – (Washington) **State fines DOE \$50,000 for mishandling waste at Hanford plant.** The Washington State Department of Ecology fined the U.S. Department of Energy (DOE) and its contractor, CH2M Hill Plateau Remediation Co., \$50,000 August 9 for mishandling waste at the Hanford Site's T Plant including containers holding leaking batteries, paint chips, grease, and concrete pieces that had the potential to include low levels of radioactive contamination. State officials stated the DOE and its contractor must obtain a detailed analysis of waste before storing it and properly maintain storage records.

Source: <http://www.tri-cityherald.com/news/local/hanford/article94660852.html>

## Critical Manufacturing Sector

Nothing to report

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

4. *August 9, Orange County Register* – (National) **Brea man pleads guilty in \$9 million**

**mortgage modification scheme.** The former owner and operator of California-based Rodis Law Group pleaded guilty August 9 for his role in a \$9 million fraudulent mortgage modification scheme where he and co-conspirators convinced over 1,500 struggling homeowners to pay for fraudulent services from the Rodis Law Group by falsely claiming the firm consisted of a team of attorney's experienced in negotiating lower principal balances and interest rates on mortgage loans, among other misrepresentations from October 2008 – June 2009. Two other co-conspirators have pleaded guilty for their roles in the scheme.

Source: <http://www.ocreger.com/articles/antonio-725190-rodis-law.html>

For another story, see item [24](#)

## **Transportation Systems Sector**

5. *August 9, St. Joseph News-Press* – (Missouri) **Concrete truck overturns near San Jose steak house.** U.S. Highway 169 in St. Joseph, Missouri, was closed for several hours August 9 while crews worked to remove the wreckage from a two-vehicle crash after a semi-truck hit a truck carrying concrete, causing the concrete truck to overturn. No injuries were reported.  
Source: [http://www.newspressnow.com/news/local\\_news/article\\_72e530d4-b91b-58fc-9840-c933981dbde4.html](http://www.newspressnow.com/news/local_news/article_72e530d4-b91b-58fc-9840-c933981dbde4.html)
6. *August 9, KREM 2 Spokane* – (Washington) **Spilled gravel block both lanes of Hwy 27 in Palouse.** A semi-truck overturned and spilled its load of gravel blocking both lanes of Highway 27 in Palouse, Washington, for several hours August 9. No injuries were reported.  
Source: <http://www.krem.com/news/traffic/spilled-gravel-block-both-lanes-of-hwy-27-in-palouse/292358397>
7. *August 9, WXII 12 Winston-Salem*– (North Carolina) **1 killed in crash that closed Highway 52 in Winston-Salem.** Highway 52 in Winston-Salem, North Carolina, was closed for more than 2 hours August 9 while crews worked to clear the wreckage from a single-vehicle crash that killed one person.  
Source: <http://www.wxii12.com/news/crash-closes-highway-52-in-winstonsalem/41115928>
8. *August 9, Santa Rosa Press Democrat* – (California) **Multicar pileup closes Highway 101 in Petaluma.** A seven-vehicle crash prompted officials to close Highway 101 in Petaluma, California, for nearly 3 hours August 9 while crews worked to clear the wreckage. Four people were transported to area hospitals with injuries.  
Source: <http://www.petaluma360.com/news/5949057-181/multicar-pileup-closes-highway-101?artslide=0>
9. *August 9, Austin American-Statesman* – (Texas) **DPS officials ID man killed in collision of U.S. 290 in Elgin.** A fatal two-vehicle crash involving a semi-truck and another vehicle closed westbound lanes of U.S. 290 in Elgin, Texas, for nearly 3 hours August 9 while officials investigated the cause of the crash and crews worked to clear

the wreckage.

Source: <http://www.statesman.com/news/news/traffic/westbound-us-290-shut-down-between-elgin-mcdade-af/nsCZ4/>

10. *August 9, Mankato Free Press* – (Minnesota) **Six injured in crash near St. Peter.** Highway 99 near St. Peter, Minnesota, was closed for several hours August 9 while officials investigated the scene of a two-vehicle crash that injured six people.  
Source: [http://www.mankatofreepress.com/news/local\\_news/crash-under-investigation-near-st-peter/article\\_cf768150-5e47-11e6-b0b7-0b7e64594da2.html](http://www.mankatofreepress.com/news/local_news/crash-under-investigation-near-st-peter/article_cf768150-5e47-11e6-b0b7-0b7e64594da2.html)
11. *August 8, WTOP 103.5 FM Washington, D.C.* – (Washington, D.C.; Maryland) **Post-derailment Metro inspections prompt major Red Line weekend shutdown.** Washington Metropolitan Area Transit Authority (WMATA) officials announced August 8 that there will be no train service on the Red Line at the Shady Grove, Rockville, Twinbrook, and White Flint stations August 13 – August 14 after new inspections were ordered following a July derailment at the Twinbrook station.  
Source: <http://wtop.com/tracking-metro-24-7/2016/08/post-derailment-metro-inspections-prompt-major-red-line-weekend-shutdown/>

## **Food and Agriculture Sector**

12. *August 9, U.S. Department of Labor* – (Pennsylvania) **OSHA finds Pennsylvania feed mill ignored previously identified severe combustible dust, grain-handling hazards, while dangers remain.** The Occupational Safety and Health Administration cited Mattocks Five Inc., doing business as Albion Mill with 5 willful, 9 repeat, 1 other-than-serious, and 12 serious safety and health violations August 1 following a February inspection at the company's Albion, Pennsylvania facility which revealed that the company failed to develop a housekeeping program to prevent worker exposure to combustible dust hazards, failed to properly store propane cylinders, and failed to prevent electrical hazards, among other violations. Proposed penalties total \$195,460.  
Source:  
[https://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=32985](https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32985)

## **Water and Wastewater Systems Sector**

13. *August 8, Kitsap Sun* – (Washington) **Sewage spill closes waters near Keyport.** The Kitsap Public Health District issued a 3-day no-contact advisory for a stretch of Liberty Bay from Lemolo Point to Point Bolin and Nesika Bay August 8 after about 2,000 gallons of sewage spilled from a Kitsap County-managed waste water facility near the Keyport boat ramp in Keyport, Washington.  
Source: <http://www.kitsapsun.com/news/local/sewage-spill-closes-waters-near-keyport-39982d85-355d-0808-e053-0100007fc1c5-389543821.html>
14. *August 8, U.S. Environmental Protection Agency* – (Hawaii) **EPA enforces ban on cesspools on Big Island and Maui.** The U.S. Environmental Protection Agency (EPA) announced three separate agreements with the County of Hawaii, the County of Maui,

and the State of Hawaii Department of Land and Natural Resources (DLNR) August 8 to close cesspools on Maui and the Big Island after the EPA discovered the counties were violating a Federal ban on large capacity cesspools. Under the agreements, the County of Hawaii will pay a \$105,000 fine for its two cesspools, the County of Maui will pay \$33,000 for their cesspool at the Maui Raceway Track, and the DLNR will pay a \$50,000 fine for their cesspools at Waianapanapa State Park, as well as close or convert smaller cesspools at 7 State parks and recreation areas.

Source: <https://www.epa.gov/newsreleases/epa-enforces-ban-cesspools-big-island-and-maui>

## **Healthcare and Public Health Sector**

15. *August 9, U.S. Department of Justice* – (Florida) **Eight individuals charged in multimillion-dollar compounding pharmacy fraud scheme.** Eight Florida residents were charged in an indictment unsealed August 9 for their roles in a multi-million dollar health care fraud scheme where the group allegedly used the A to Z Pharmacy Inc., in New Port Richey and several Miami-area pharmacies to submit nearly \$663 million in fraudulent reimbursement claims for prescription compounded medications to private insurance companies, Medicare and Tricare, and received approximately \$157 million in reimbursement claims from October 2012 – December 2015 that were based on prescriptions generated as a result of kickbacks and bribes. The charges also allege that the group used shell companies to transfer and distribute the money and conceal the fraudulent activities.

Source:

<https://www.justice.gov/opa/pr/eight-individuals-charged-multimillion-dollar-compounding-pharmacy-fraud-scheme>

## **Government Facilities Sector**

16. *August 9, KPIX 5 San Francisco; Associated Press* – (California) **Big Sur wildfire grows to more than 100 square miles.** More than 5,000 firefighters reached 50 percent containment August 9 of the 67,092-acre Soberanes Fire burning in Big Sur, California, which has destroyed 57 homes and prompted the closure of 5 State parks on Highway 1 between San Francisco and Los Angeles.

Source: <http://sanfrancisco.cbslocal.com/2016/08/09/big-sur-soberanes-wildfire-104-square-miles/>

17. *August 9, Elko Daily Free Press* – (Nevada) **Overland Fire burns 8,900 acres in south Ruby Mountains.** Crews worked August 9 to contain the 8,900-acre Overland Fire burning in the south Ruby Mountains in Nevada. Crews also worked August 9 to contain the Strawberry Fire burning in Great Basin National Park which has burned between 3,000 and 5,000 acres and prompted the closure of portions of the park, including Wheeler Peak Campground.

Source: [http://elkodaily.com/news/local/south-ruby-fire-grows-another-big-blaze-at-great-basin/article\\_ad8decba-565f-5511-b17a-46cc7f236447.html](http://elkodaily.com/news/local/south-ruby-fire-grows-another-big-blaze-at-great-basin/article_ad8decba-565f-5511-b17a-46cc7f236447.html)

18. *August 9, KABC 7 Los Angeles* – (California) **Pilot Fire spreads to 7,736 acres near**

**Silverwood Lake.** Approximately 1,475 firefighters worked August 9 to contain the 7,736-acre Pilot Fire burning in the San Bernardino National Forest in California which has forced the evacuation of over 4,700 homes, threatens 5,300 structures, closed roads in the area, and prompted the closure of the Apple Valley School District until August 11.

Source: <http://abc7.com/news/pilot-fire-spreads-to-6963-acres-near-silverwood-lake/1462634/>

## **Emergency Services Sector**

Nothing to report

## **Information Technology Sector**

19. *August 10, Softpedia* – (International) **Data of nearly 2 million users exposed in Dota2 forum hack.** Researchers from LeakedSource reported that the Dota2 official developers forum was breached after hackers stole the usernames, email addresses, user identifiers, passwords, and IP addresses of nearly 2 million of the forum's users July 10 by hashing and salting the password with the MD5 algorithm. Forum administrators patched the vulnerability and reset all user account passwords.  
Source: <http://news.softpedia.com/news/data-of-nearly-2-million-users-exposed-in-dota2-forum-hack-507162.shtml>
20. *August 10, SecurityWeek* – (International) **Microsoft patches flaws in Windows, Office, browsers.** Microsoft released 9 security bulletins patching a total of 27 important and critical vulnerabilities including 9 critical vulnerabilities in Internet Explorer and 8 critical flaws in Edge that can be exploited for remote code execution and information disclosure by tricking a targeted user into visiting a malicious Website, remote code execution issues in Windows, Office, Skype for Business and Lync caused by the way Windows font library handles specially crafted embedded fonts, and critical flaws in Office that can be leveraged for remote code execution if a victim opens a malicious file, among other vulnerabilities.  
Source: <http://www.securityweek.com/microsoft-patches-flaws-windows-office-browsers>
21. *August 10, SecurityWeek* – (International) **Juniper starts fixing IPv6 processing vulnerability.** Juniper Networks released hotfixes for its JUNOS F3 and F2 products resolving a vulnerability in its JUNOS and Junos routers after Cisco researchers discovered the flaw can be exploited to cause a denial-of-service (DoS) condition by sending a flood of specially crafted IPv6 Neighbor Discovery (ND) packets from non-link-local sources to affected devices in order to fill up the packet processing queue and cause legitimate IPv6 ND packets to drop. The company was working to release patches for the issue.  
Source: <http://www.securityweek.com/juniper-starts-fixing-ipv6-processing-vulnerability>
22. *August 9, Softpedia* – (International) **Researchers hide malware inside digitally**



**signed files without breaking hashes.** Security researchers from Deep Instinct discovered attackers could inject malware inside a digitally signed binary without affecting the overall file hash after finding that Microsoft Windows does not include three fields from a file's Portable Executable (PE) headers during the file hash validation process and that modifying these fields does not break the certificate's validity, allowing the malicious files to avoid detection by security and antivirus software. Researchers stated the technique does not require attackers to hide the malicious code via packers and bypasses any secondary checks of security software. Source: <http://news.softpedia.com/news/researchers-hide-malware-inside-digitally-signed-files-without-breaking-hashes-507146.shtml>

23. *August 9, SecurityWeek* – (International) **Go-based Linux trojan used for cryptocurrency.** Doctor Web researchers reported that a new Linux trojan, dubbed Linus.Lady.1 allows hackers to earn a profit by exploiting infected systems for cryptocurrency mining after finding that the trojan collects information on an infected machine, including the operating system, central processing unit (CPUs), and processes, and sends the harvested data back to a command and control (C&C) server, which then provides a configuration file for downloading a cryptocurrency mining application designed for Monero (XMR) mining. Researchers also found the trojan is capable of spreading to other Linux computers on an infected network by connecting to remote hosts over port 6379 without a password and downloading a script from a specified Uniform Resource Locator (URL) which is responsible for downloading and installing a copy of the trojan. Source: <http://www.securityweek.com/go-based-linux-trojan-used-cryptocurrency-mining>

For another story, see item [24](#)

### 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

Nothing to report

## Commercial Facilities Sector

24. *August 9, Softpedia* – (International) **Criminal group uses LogMeIn to compromise PoS systems with malware.** Researchers from PandaLabs discovered a criminal group was using compromised LogMeIn accounts belonging to systems running point-of-sale (PoS) software and connected to PoS terminals to access over 200 devices and infect them with the PunkeyPOS, Multigrain, or PosCardStealer malware. The researchers reported that the hackers exploited weak login credentials or discovered the login

credentials from other sources.

Source: <http://news.softpedia.com/news/criminal-group-uses-logmein-to-compromise-pos-systems-with-malware-507112.shtml>

25. *August 9, KFMB 8 San Deigo* – (California) **City Heights apartment fire leads to evacuations.** A 2-alarm fire at a City Heights apartment complex August 9 forced 41 residents to evacuate, left 6 people injured, and caused an estimated \$325,000 in damage after a resident was smoking while using an oxygen tank, causing the fire to ignite.

Source: <http://www.cbs8.com/story/32716866/city-heights-apartment-fire-leads-to-evacuations>

## **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 <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.