



## Daily Open Source Infrastructure Report 08 April 2015

### Top Stories

- Officials announced a \$225 million settlement April 6 between Exxon Mobil and New Jersey for contamination at more than 16 refineries and other polluted sites across the State. – *Newark Star-Ledger* (See item [1](#))
- A Montana man pleaded guilty April 3 for his role in a cramming scheme that involved adding \$70 million in unauthorized charges onto customers’ phone bills nationwide. – *Associated Press* (See item [25](#))
- The U.S. Federal Communications Commission issued CenturyLink Inc., \$16 million in penalties and fined Intrado \$1.4 million for a 9-1-1 emergency call service outage that lasted 6 hours and affected 11 million people across 11 States in 2014. – *Denver Business Channel* (See item [27](#))
- A 4-alarm fire destroyed or severely damaged 60 businesses in the Pecan Park Flea & Farmers’ Market in Jacksonville, Florida, April 6. – *WJXX 25 Orange Park/WLTV 12 Jacksonville* (See item [29](#))

---

### 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. *April 7, Newark Star-Ledger* – (New Jersey) **New details in \$225M Exxon pollution settlement made public today.** New Jersey officials announced a \$225 million settlement April 6 between Exxon Mobil and the State for contamination at more than 16 refineries and other polluted sites across New Jersey. The oil company agreed to pay out in the settlement which also clears the company for liability for pollution at the sites.  
Source: [http://www.nj.com/news/index.ssf/2015/04/historic\\_settlement\\_with\\_exxon\\_includes\\_polluted\\_r.html](http://www.nj.com/news/index.ssf/2015/04/historic_settlement_with_exxon_includes_polluted_r.html)
2. *April 7, Columbus Dispatch* – (National) **Two coal plants in Ohio part of AEP closings.** American Electric Power will close 7 coal-fired power plants and convert 2 others to run on natural gas in Ohio, Virginia, West Virginia, Kentucky, and Indiana by the end of May as part of plans announced in 2011, and required in part by federal clean-air rules.  
Source: <http://www.dispatch.com/content/stories/business/2015/04/07/two-coal-plants-in-ohio-part-of-closings.html>
3. *April 6, Chico Enterprise-Record* – (California) **About 79,000 customers lose power in Butte County.** A widespread power outage in Chico and surrounding areas knocked out electricity to 79,000 customers in Butte County, prompting the closure of Chico State University for nearly 8 hours and the closure of the Chico Mall. Pacific Gas and Electric Co., reported that the outage resulted from a failure of a 500-kilovolt line near Table Mountain.  
Source: <http://www.redding.com/news/local-news/about-79000-customers-lose-power-in-butte-county>
4. *April 6, U.S. Securities and Exchange Commission* – (National) **SEC charges California companies with running a \$33 million oil and gas scheme.** Team Resources, Inc., Fossil Energy Corp., 4 sales associates, and the principal were charged by the U.S. Securities and Exchange Commission April 6 for raising more than \$33 million from approximately 475 investors nationwide through 8 unregistered offerings of oil-and-gas partnership interests from 2007 through 2012. The companies would cold-call potential investors and mislead them about information such as potential returns, success of past offers, and how offering proceeds would be used in order to convince them to purchase partnership interests.  
Source: <http://www.sec.gov/litigation/litreleases/2015/lr23230.htm>

[\[Return to top\]](#)

## Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

## Nuclear Reactors, Materials, and Waste Sector

5. *April 6, Monroe News* – (Michigan) **Fermi 2 back online after water leak.** Officials at DTE Energy confirmed that the Fermi 2 nuclear power plant in Frenchtown Township was running at 100 percent power April 6 after the reactor automatically shut down March 19 when monitoring systems detected a leak in the system that cools various heat exchanges separate from the reactor. Maintenance crews repaired the leak and other equipment and began synchronizing the plant April 4 before returning it to full capacity.

Source: <http://www.monroenews.com/news/2015/apr/06/fermi-2-back-online-after-water-leak/>

[\[Return to top\]](#)

## Critical Manufacturing Sector

Nothing to report

[\[Return to top\]](#)

## Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

## Financial Services Sector

6. *April 7, Softpedia* – (International) **Word documents with scrambled text deliver banking trojan in the background.** Security researchers from Cisco's Talos research group discovered a new variant of the Dridex banking trojan being delivered via incomprehensible malware-laden Microsoft Word documents that trick users into enabling macros before using PowerShell to download and execute the trojan from a hard-coded IP address. The malware campaign lasted for less than 5 hours before antivirus solutions responded.

Source: <http://news.softpedia.com/news/Word-Documents-with-Scrambled-Text-Deliver-Banking-Trojan-in-the-Background-477781.shtml>

For additional stories, see items [24](#) and [25](#)

[\[Return to top\]](#)

## Transportation Systems Sector

7. *April 7, Bluefield Daily Telegraph* – (West Virginia) **Fuel tanker crashes.** A stretch of U.S. Route 52 in McDowell County was closed for about 7 hours April 6 due to a fuel leak from an overturned semi-truck that crashed near Eckman. A HAZMAT crew

responded to help clear the scene, and the driver of the semi-truck was extricated and transported to an area hospital.

Source: [http://www.bdtonline.com/news/fuel-tanker-crashes/article\\_1ab653c6-dcd9-11e4-93a6-3be3570db740.html](http://www.bdtonline.com/news/fuel-tanker-crashes/article_1ab653c6-dcd9-11e4-93a6-3be3570db740.html)

8. *April 7, San Francisco Bay Area News* – (California) **Fremont: Lanes cleared after big-rig crash on I-680.** Northbound lanes of Interstate 680 in Fremont were closed for about 3 hours April 7 while crews cleared the scene of an accident involving a semi-truck that blocked the roadway. No injuries were reported in the crash.  
Source: [http://www.mercurynews.com/crime-courts/ci\\_27863971/chp-big-rig-blocking-lanes-i-680-fremont](http://www.mercurynews.com/crime-courts/ci_27863971/chp-big-rig-blocking-lanes-i-680-fremont)
9. *April 7, Sacramento Bee* – (California) **Lanes are clear after two big rig crashes snarl morning traffic on I-5.** Interstate 5 in downtown Sacramento was closed for several hours April 7 while crews cleared the scene of 2 separate semi-truck accidents. HAZMAT crews responded to the scene of one of the incidents where about 125 gallons of diesel fuel spilled onto the freeway from a United Parcel Service semi-truck.  
Source: <http://www.sacbee.com/news/local/crime/article17616416.html>
10. *April 6, Washington Post* – (Virginia) **NTSB looking at second Metro incident as part of tunnel-smoke probe.** The National Transportation Safety Board (NTSB) stated April 6 that it will investigate a February 11 incident inside a tunnel of the Washington Metropolitan Area Transit Authority's Metro system where an occurrence of smoke and an electrical malfunction forced a train to reverse and return to the Court House station in Virginia, causing a 1-hour service disruption while smoke cleared from the tunnel. The investigation will consider similarities to a fatal incident near the L'Enfant Plaza Metro station in January that remains under NTSB investigation.  
Source: [http://www.washingtonpost.com/local/trafficandcommuting/ntsb-looking-at-feb-11-incident-for-clues-in-fatal-lenfant-smoke-incident/2015/04/06/203c6a0e-dc95-11e4-a500-1c5bb1d8ff6a\\_story.html](http://www.washingtonpost.com/local/trafficandcommuting/ntsb-looking-at-feb-11-incident-for-clues-in-fatal-lenfant-smoke-incident/2015/04/06/203c6a0e-dc95-11e4-a500-1c5bb1d8ff6a_story.html)

[\[Return to top\]](#)

## **Food and Agriculture Sector**

11. *April 7, Upper Valley News* – (Vermont) **Cause of Britton Lumber sawmill fire left 'undetermined'.** Vermont State Police fire investigators reported April 6 that they were unable to determine the cause of a March 28 fire that destroyed the Britton Lumber Company's sawmill in Fairlee. The sawmill was taken out of operation indefinitely, and the company was working to acquire enough lumber to continue supplying customers until the sawmill is repaired.  
Source: <http://www.vnews.com/news/16403955-95/cause-of-britton-lumber-sawmill-fire-left-undetermined>
12. *April 6, WAVY 10 Portsmouth* – (Virginia) **York River shellfish harvesting banned after sewage spill.** The Virginia Department of Health announced April 6 an emergency ban of shellfish harvesting from a section of the York River from April 6

through April 28 after a pipe broke and caused a significant spill of raw sewage into Wormley Creek, which feeds into the river.

Source: <http://wavy.com/2015/04/06/york-river-shellfish-harvesting-banned-after-sewage-spill/>

13. *April 6, Reuters* – (Minnesota) **Minnesota finds lethal bird flu in two more turkey flocks.** The U.S. Department of Agriculture (USDA) confirmed April 6 the presence of the lethal H5N2 strain of avian flu in a 26,000 turkey flock in Kandiyohi County and a 76,000 turkey flock in Stearns County, a previously established quarantine zone. Both flocks were ordered to be culled in an effort to prevent the virus from spreading, and the USDA reported that the birds will not enter the food supply.

Source: <http://www.msn.com/en-us/news/us/minnesota-finds-lethal-bird-flu-in-two-more-turkey-flocks/ar-AAauAVj>

[\[Return to top\]](#)

## **Water and Wastewater Systems Sector**

14. *April 7, WSAZ 3 Huntington* – (West Virginia) **Water restored to majority of Boone County residents.** West Virginia America Water reported April 7 that service was restored to approximately 4,600 customers in Boone County following a water main break the week of March 30 that prompted the emergency shut off of water for repairs April 5. A precautionary boil advisory was issued while crews worked to restore service to the remaining 100 customers in the area.

Source: <http://www.wsaz.com/home/headlines/Planned-Water-Outage-to-Affect-WVAW-Customers-in-Boone-County-WVa-298726161.html>

15. *April 7, Reuters* – (Louisiana) **Oil spill shuts part of Mississippi River after vessels collide.** A 9-mile stretch of the Mississippi River was closed April 6 following a collision between a ship and a vessel offloading crude in southern Louisiana that caused about 420 gallons of oil to spill into the river.

Source: <http://www.reuters.com/article/2015/04/07/us-usa-mississippi-shipping-idUSKBN0MY07620150407>

For another story, see item [12](#)

[\[Return to top\]](#)

## **Healthcare and Public Health Sector**

16. *April 7, Toledo Blade* – (Ohio) **Indictment in patient records breach.** Authorities charged a former respiratory therapist at ProMedica Bay Park Hospital in Ohio for allegedly illegally accessing the medical and personal records of 596 patients between May 2013 and March 2014 by using a protected computer without authorization. Patients were notified of the breach in May 2014.

Source: <http://www.toledoblade.com/local/2015/04/07/Indictment-in-patient-records-breach.html>

17. *April 6, KTRK 13 Houston* – (Texas) **Men accused of running illegal men’s health clinic.** Two men were charged April 6 for allegedly running Men’s Health Centers in Houston, an unlicensed clinic that was supplying patients with pills and administering injections. Authorities shut down the clinic after learning that the men had no medical background and were running the unlicensed clinic.  
Source: <http://abc13.com/news/men-accused-of-running-illegal-mens-clinic/634404/>
18. *April 4, Porterville Recorder* – (California) **County agency reports data breach.** The Tulare County Health and Human Services Agency reported that a potential breach occurred March 19 when an employee sent an unencrypted email and did not blind copy recipients of the email, potentially exposing the protected health information of 845 patients from the Visalia and Farmersville clinics that use the online Patient Portal. Officials stated that no health information was disclosed but email addresses of affected patients were visible to everyone copied on the email, which prompted the disabling of all impacted Patient Portal accounts.  
Source: [http://www.recorderonline.com/features/health\\_news/county-agency-reports-data-breach/article\\_65b3c61a-dae5-11e4-a14e-af4be86a2aa1.html](http://www.recorderonline.com/features/health_news/county-agency-reports-data-breach/article_65b3c61a-dae5-11e4-a14e-af4be86a2aa1.html)

[\[Return to top\]](#)

## **Government Facilities Sector**

19. *April 7, WKYT 27 Lexington* – (Kentucky) **Hundreds of EKV students evacuate dorm after sprinkler floods building.** Hundreds of students from Eastern Kentucky University’s Clay Hall in Richmond were evacuated for approximately 4 hours April 7 after four floors were flooded possibly due to a malfunctioning sprinkler.  
Source: <http://www.wkyt.com/home/headlines/Hundreds-of-EKV-students-evacuate-dorm-after-sprinkler-malfunction-298864241.html>
20. *April 6, Riverside Press-Enterprise* – (California) **UCR data breach affects 8,000.** University of California, Riverside officials announced April 6 that it notified 8,000 graduate students and applicants of a March 13 burglary where thieves stole a desktop computer containing the Social Security numbers of the students and potential students from the campus’ graduate division offices. The university stated that there was no evidence that the personal information was misused.  
Source: <http://www.pe.com/articles/information-764066-computer-lovekin.html>

For another story, see item [3](#)

[\[Return to top\]](#)

## **Emergency Services Sector**

21. *April 7, WTTG 5 Washington, D.C.* – (Maryland) **2 fire trucks destroyed in 3-alarm fire in Capitol Heights.** An April 6 fire that began outside a roofing business in Capitol Heights, Maryland, destroyed two fire trucks worth over \$1.5 million. The fire left minor smoke damage to the roof of the building and officials believe that exploding

propane tanks helped destroy the two fire engines.

Source: <http://www.myfoxdc.com/story/28733345/fire-capitol-heights>

For another story, see item [27](#)

[\[Return to top\]](#)

## **Information Technology Sector**

22. *April 7, Help Net Security* – (International) **New crypto-ransomware “quarantines” files, downloads info-stealer.** Security researchers at Trend Micro discovered a new piece of crypto-ransomware dubbed CryptVault that uses open-source GnuPG to create RSA-1024 public and private key pairs that encrypt files to make them resemble files quarantined by an anti-virus solution, before asking for ransom and downloading and executing Browser Password Dump to extract passwords stored by Web browsers. Attackers spread the malware by tricking users into running malicious Javascript file attachments.

Source: [http://www.net-security.org/malware\\_news.php?id=3008](http://www.net-security.org/malware_news.php?id=3008)

23. *April 7, Softpedia* – (International) **Dell System Detect flagged as a risk by antivirus product.** Malwarebytes added Dell’s System Detect tool to its list of potentially unwanted applications (PUP) due to a serious remote code execution vulnerability in older versions that attackers could exploit by initiating requests from Web sites containing a “dell” string to download and launch files following an easily bypassed authentication process. Dell mitigated the vulnerability in an update released during the week of March 30.

Source: <http://news.softpedia.com/news/Dell-System-Detect-Flagged-as-a-Risk-by-Antivirus-Product-477811.shtml>

24. *April 6, Softpedia* – (International) **Angler Exploit Kit now relies on more successful infection tactics.** Security researchers from Zscaler’s Threat Lab identified an evolution in the Angler Exploit Kit (EK) in which attackers are utilizing 302 Cushioning and domain shadowing as infection vectors, in addition to typical malvertising that targets users with outdated browser plug-ins. Researchers believe that the malware dropped by Angler EK in recent attacks was a Carberp family banking trojan.

Source: <http://news.softpedia.com/news/Angler-Exploit-Kit-Now-Relies-on-More-Successful-Infection-Tactics-477736.shtml>

For another story, see item [6](#)

### **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>

[\[Return to top\]](#)

## **Communications Sector**

25. *April 6, Associated Press* – (National) **Man pleads guilty in phone ‘cramming’ case.** A Montana man pleaded guilty April 3 for his role in a cramming scheme that involved adding \$70 million in unauthorized charges onto customers’ phone bills nationwide through answering questions on Web sites offering free products or job-search assistance. A U.S. Federal Trade Commission investigation was initiated after consumers began complaining about erroneous charges on their monthly bills, prompting the commission to bring civil action against the man, his son, wife, accountant, and nine companies in 2013.  
Source: <http://www.greatfalltribune.com/story/news/crime/2015/04/06/man-pleads-guilty-phone-cramming-case/25367601/>
26. *April 6, U.S. Securities and Exchange Commission* – (National) **SEC charges firms and individuals for defrauding investors in cellular licensing scheme.** The U.S. Securities and Exchange Commission charged 12 companies and 6 individuals April 6 for defrauding investors of more than \$12.4 million from May 2012 – October 2014 in a scheme involving applications to the U.S. Federal Communications Commission for cellular spectrum licenses. The accused allegedly engaged in the unregistered offer and sale of securities and misrepresented the value and use of certain cellular spectrum licenses in the 800 megahertz band.  
Source: <http://www.sec.gov/news/pressrelease/2015-57.html>
27. *April 6, Denver Business Journal* – (National) **CenturyLink, Colorado's Intrado fined by FCC over 911 outage.** The U.S. Federal Communications Commission (FCC) issued CenturyLink Inc., \$16 million in penalties and fined Intrado \$1.4 million for a 9-1-1 emergency call service outage that lasted 6 hours and affected 11 million people across 11 States in 2014. An FCC investigation determined that the outage was due to a preventable technical outage and resulted in 6,600 missed 9-1-1 calls.  
Source: [http://www.bizjournals.com/denver/blog/boosters\\_bits/2015/04/centurylink-coloradosintrado-fined-by-fcc-over-911.html?page=all](http://www.bizjournals.com/denver/blog/boosters_bits/2015/04/centurylink-coloradosintrado-fined-by-fcc-over-911.html?page=all)

[\[Return to top\]](#)

## **Commercial Facilities Sector**

28. *April 7, Duluth News Tribune* – (Minnesota) **Duluth apartment fire still smoldering; dozens left homeless.** Duluth firefighters worked April 6 to contain an April 5 fire that destroyed the Applewood Knoll apartments, left 44 residents displaced, and caused over \$900,000 in damages. Two people were transported to an area hospital and the cause of the fire is under investigation.  
Source: <http://www.duluthnewstribune.com/news/3716205-duluth-apartment-fire-still-smoldering-dozens-left-homeless>
29. *April 7, WJXX 25 Orange Park/WLTV 12 Jacksonville* – (Florida) **4-alarm fire engulfs**



**Pecan Park Flea Market.** A 4-alarm fire destroyed or severely damaged 60 businesses in the Pecan Park Flea & Farmers' Market in Jacksonville, Florida, April 6. Crews remained at the scene April 7 to put out hot spots and investigate the cause of the fire and the extent of damages.

Source: <http://www.firstcoastnews.com/story/news/local/2015/04/06/fire-three-alarm-pecan-park-flea-market/25393905/>

30. *April 6, KMGH 7 Denver* – (Colorado) **White powder sent to Jewish Community Center, synagogue in Boulder tested, deemed not dangerous.** A letter containing an unknown white powder prompted the evacuation of the Jewish Community Center in Boulder and the quarantine of employees who opened the envelope April 6 before authorities were able to test the substance and deem it to be safe. A second envelope containing white powder was sent to the Congregation Har HaShem in Boulder, which was also deemed harmless.

Source: <http://www.thedenverchannel.com/news/local-news/white-powder-sent-to-boulder-jcc-in-threatening-letter>

For additional stories, see items [3](#) and [21](#)

[\[Return to top\]](#)

## **Dams Sector**

Nothing to report

[\[Return to top\]](#)



**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.