



Daily Open Source Infrastructure Report 22 May 2015

Top Stories

- Transocean Ltd., reached a settlement May 20 with the Plaintiffs Steering Committee for nearly \$211.8 million involving 2 classes of businesses and individuals following the April 2010 drilling rig accident that killed 11 workers and released oil into the Gulf of Mexico for 87 days. – *Associated Press* (See item [1](#))
- ConAgra Foods agreed May 20 to pay \$11.2 million to settle a 2007 Federal charge after traces of Salmonella were found in Peter Pan peanut butter produced at the company’s Sylvester, Georgia plant, resulting in at least 625 illnesses. – *Associated Press* (See item [7](#))
- Miami-Dade police arrested 5 individuals May 20 for their alleged involvement in a pharmaceutical drug crime ring that netted approximately \$6.5 million. – *WPLG 10 Miami* (See item [13](#))
- CareFirst BlueCross BlueShield announced May 20 that 1.1 million clients in Maryland, Virginia, and Washington, D.C., had their personal information accessed in a June 2014 cyberattack on the health insurer’s Web site. – *Washington Post* (See item [14](#))

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. *May 20, Associated Press* – (National) **A series of settlements in 2010 Gulf oil spill.** Transocean Ltd., the owner of the Deepwater Horizon drilling rig, reached a settlement May 20 with the Plaintiffs Steering Committee for nearly \$211.8 million involving 2 classes of businesses and individuals following the April 2010 drilling rig accident that killed 11 workers and released oil into the Gulf of Mexico for 87 days. BP, which leased the rig from Transocean, reached separate settlements with Transocean and the Halliburton Company.

Source: <http://news.yahoo.com/211m-settlement-reached-transocean-2010-oil-spill-215129824--finance.html>

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

Chemical Industry Sector

Nothing to report

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

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

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

Critical Manufacturing Sector

2. *May 20, Detroit Free Press* – (Michigan) **Dearborn steel plant to pay \$1.35M fine to settle alleged violations.** The U.S. Department of Justice, the Federal government, and the State of Michigan reached a settlement May 20 with AK Steel resolving 42 violations, including 2 notices issued by the U.S. Environmental Protection Agency against the Dearborn plant's previous owner, Severstal North America. The company will pay \$1.35 million in fines, as well as implement procedures to reduce Clean Air Act violations, and install air filtration systems at Salina schools near the plant.

Source: <http://www.freep.com/story/news/local/2015/05/20/steel-plant-penalty/27646815/>

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

Defense Industrial Base Sector

Nothing to report

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

Financial Services Sector

3. *May 20, Miami Herald* – (Florida) **31 arrested in organized insurance fraud scheme.** Miami-Dade officials announced the arrest of 31 people May 20, involved in an alleged insurance fraud scheme that bilked insurance companies in Florida out of more than \$7 million by intentionally setting fires and causing floods in homes across the State. Investigators reported that the individuals involved managed to stage 20 fires and 5 floods between 2011 and 2013 after being introduced to the homeowners through recruiters.

Source:

<http://www.miamiherald.com/news/local/community/broward/article21530616.html>

For additional stories, see items [21](#) and [26](#)

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

Transportation Systems Sector

4. *May 20, WCAU 10 Philadelphia* – (International) **Passenger on board Philadelphia to Frankfurt plane dies.** An American Airlines flight headed from Philadelphia to Frankfurt, Germany, made an emergency landing in Gander International Airport in Canada May 20 due to a medical emergency on board. The flight was canceled after the passenger died and remaining passengers were forced to stay at a nearby hotel overnight until a new plane arrived.

Source: <http://www.nbcphiladelphia.com/news/local/Passenger-Philadelphia-to-Frankfurt-Plane-Dies-Gander-Diversion-304386051.html>

5. *May 20, WPDE 15 Florence* – (South Carolina) **Wreck shuts down southbound U.S. 17 Bypass.** Southbound lanes of U.S. 17 Bypass in Myrtle Beach were closed for more than 7 hours May 20 while officials responded to a 6-vehicle accident that injured 1 person. The cause of the crash remains under investigation.

Source: <http://www.carolinalive.com/news/story.aspx?id=1207205>

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

Food and Agriculture Sector

6. *May 21, Food Safety News* – (Wisconsin) **60 now sickened in WI Salmonella outbreak linked to grocery store.** Health officials in Kenosha County, Wisconsin, are investigating over 60 Salmonella illnesses allegedly connected to meat consumption from the Supermercado Los Corrales grocery store. Authorities reported May 19 that the meat and food preparation area is temporarily closed while the source of the outbreak remains under investigation.

Source: <http://www.foodsafetynews.com/2015/05/salmonella-outbreak-in-wisconsin-sickens-at-least-20>

7. *May 20, Associated Press* – (Georgia) **ConAgra to pay \$11.2 million to settle charge**

over tainted peanut butter. Omaha-based ConAgra Foods agreed May 20 to pay \$11.2 million to settle a 2007 Federal charge after traces of Salmonella were found in Peter Pan peanut butter produced at the company's Sylvester, Georgia plant, resulting in at least 625 illnesses across 47 States. Company officials reported that moisture from a leaky roof and a malfunctioning sprinkler system allowed Salmonella bacteria to grow on raw peanuts.

Source: http://www.omaha.com/money/conagra-to-pay-million-to-settle-charge-over-tainted-peanut/article_c48f928c-ff0b-11e4-a067-4f113d778f28.html

8. *May 20, U.S. Department of Agriculture* – (National) **LQNN, Inc. recalls poultry, beef and pork products produced without the benefit of inspection and misbranded with unauthorized use of the USDA mark of inspection.** LQNN Inc., operating as Lee's Sandwiches of Garden Grove, California, recalled approximately 213,192 pounds of chicken, beef, and pork products May 20 that were produced and sold without the benefit of inspection and misbranded due to the unauthorized use of a U.S. Department of Agriculture mark of inspection. The products were distributed to restaurants in Arizona, California, Nevada, Oklahoma, Oregon, and Texas.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-081-2015-release>
9. *May 19, Milwaukee Journal Sentinel* – (Wisconsin) **Ag officials lift Juneau County farm's bird flu quarantine.** Wisconsin agriculture officials lifted a 6-mile quarantine zone around a Juneau County farm May 19 after no new cases of bird flu were reported in the county since the original detection in April, which affected a flock of backyard birds that were culled.
Source: <http://www.jsonline.com/news/wisconsin/ag-officials-lift-juneau-county-farms-bird-flu-quarantine-b99503707z1-304337551.html>

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

Water and Wastewater Systems Sector

10. *May 20, Mississippi News Now* – (Mississippi) **E.coli found in some Mississippi drinking water.** The Mississippi State Department of Health issued 3 boil water alerts May 20 for 3 counties affecting about 4,312 customers after E.coli bacteria was found in the drinking water systems.
Source: <http://www.wmcactionnews5.com/story/29117932/e-coli-found-in-some-mississippi-drinking-water>
11. *May 20, Associated Press* – (National) **Feds providing \$50M for Western water-saving projects.** The U.S. Government announced May 20 that it will invest nearly \$50 million in more than 60 water conservation and reuse projects in 12 drought-stricken Western States. The funding will also help pay for studies and projects that can potentially eliminate leaky open canals, create pipelines, and upgrade reclamation and water treatment plants.
Source: http://missoulian.com/news/state-and-regional/montana/feds-providing-m-for-western-water-saving-projects/article_a1929bb1-85a9-5b1d-be36-689553ad26b5.html

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

Healthcare and Public Health Sector

12. *May 21, Marin Independent Journal* – (California) **State fines Marin General Hospital \$100,000 for leaving object in patient’s skull.** The California Department of Health fined Marin General Hospital \$100,000 May 20 after a surgical team left a small plastic clip inside a patient’s skull during a procedure in August 2013. The hospital announced that it created preventative measures to help avoid future accidents, after investigators learned that the hospital did not require personnel to count the number of clips after surgery.
Source: <http://www.marinij.com/health/20150520/state-fines-marin-general-hospital-100000-for-leaving-object-in-patients-skull>
13. *May 20, WPLG 10 Miami* – (Florida) **5 arrests in fight against widespread pharmaceutical fraud in Miami-Dade.** Miami-Dade police arrested 5 individuals May 20 for their alleged involvement in a pharmaceutical drug crime ring that netted approximately \$6.5 million, and involved the group purchasing drugs from patients and reselling them to manufacturers and pharmacies.
Source: <http://www.local10.com/news/3-arrests-in-widespread-pharmaceutical-fraud-in-miamidade/33125676>
14. *May 20, Washington Post* – (Maryland; Virginia; Washington, D.C.) **Cyberattack on CareFirst exposes data on 1.1 million customers in D.C., Md. and Va.** CareFirst BlueCross BlueShield announced May 20 that 1.1 million current and former clients in Maryland, Virginia, and Washington, D.C., had their names, birth dates, email addresses, and subscriber identification numbers accessed in a June 2014 cyberattack on the health insurer’s Web site. Officials are investigating the nature and scope of the breach.
Source: <http://www.washingtonpost.com/blogs/the-switch/wp/2015/05/20/cyberattack-on-carefirst-exposes-data-on-1-1-million-customers-in-d-c-md-and-va/>
15. *May 20, Dallas Morning News* – (Texas) **Dallas anesthesiologist, indicted on 17 counts of health care fraud, to plead not guilty.** An indictment unsealed May 20 charges a Dallas-based licensed anesthesiologist for allegedly submitting at least \$5 million in phony claims to BlueCross BlueShield of Texas, United Healthcare, and the Federal Employees Health Benefits Program from 2009-2010, while falsely claiming to be present during procedures. The anesthesiologist also allegedly inflated the amount of time the procedures took and pre-signed medical records representing that the services were provided prior to the procedures taking place.
Source: <http://crimeblog.dallasnews.com/2015/05/dallas-anesthesiologist-with-garage-full-of-fancy-cars-indicted-on-17-counts-of-health-care-fraud.html/>

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

Government Facilities Sector

16. *May 21, Tucson News Now* – (Arizona) **Oak Tree fire at 2,000 acres, SR 83 open drivers urged to go slow.** Crews reached 20 percent containment May 21 of the Oak Tree Fire that grew to 2,000 acres north of Sonoita in Tucson.
Source: <http://www.tucsonnewsnow.com/story/29118854/brush-fire-causes-restrictions-on-sonoita-highway-for-2nd-straight-day>
17. *May 21, Los Angeles Daily News* – (California) **Woman in custody after saying she had a bomb at Federal Building in downtown Los Angeles.** Authorities took a suspect into custody after the Federal Building in downtown Los Angeles was evacuated for 3 hours May 20 when the suspect claimed to have explosives and threatened to blow up the building. The suspect appeared to have been suffering from a mental illness and no explosives were found.
Source: <http://www.dailynews.com/general-news/20150520/woman-in-custody-after-saying-she-had-a-bomb-at-federal-building-in-downtown-los-angeles>
18. *May 20, Columbus Dispatch* – (Ohio) **Student information exposed in Southwest Licking data breach.** Officials with the Southwest Licking School District in Ohio notified as many as 112 students May 20 that their information may have been accessed after authorities learned April 14 that a student hacked into the district's student information system and compromised the personal information of 1 student. The district continues to investigate the breach and is reviewing its security protocols.
Source: <http://www.dispatch.com/content/stories/local/2015/05/20/Southwest-Licking-data-breach.html>
19. *May 20, WMAQ 5 Chicago* – (Illinois) **CPS confirms data breach impacting 4,000 students.** Chicago Public Schools officials announced May 19 that the personally identifiable information of 4,000 students was mistakenly provided to 5 companies submitting proposals to the district. Authorities discovered the error March 24 and the five software companies confirmed that the information was destroyed.
Source: <http://www.nbcchicago.com/news/local/cps-data-breach-304367421.html>

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

Emergency Services Sector

Nothing to report

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

Information Technology Sector

20. *May 21, Securityweek* – (International) **Hundreds of cloud services potentially vulnerable to Logjam attacks: Skyhigh.** Skyhigh's Service Intelligence Team found that 575 cloud services were potentially vulnerable to attacks following the discovery of the transport layer security (TLS) vulnerability dubbed Logjam which affects a

number of cloud services. The vulnerability is caused as a result of the way the Diffie-Hellman (DHE) key exchange is deployed, and can be exploited by a man-in-the-middle (MitM) attacker to downgrade TLS connections in order to gain access to the data.

Source: <http://www.securityweek.com/hundreds-cloud-services-potentially-vulnerable-logjam-attacks-skyhigh>

21. *May 20, Softpedia* – (International) **Amount of new malware strains more than doubled in second half of 2014.** G Data researchers found that in the second half of 2014, hackers increased their malware threats as the amount of new strains grew to 125 percent, with the most prevalent being adware variants, which accounted for 31.4 percent of all threats. Researchers also determined that Vawtrak was the predominant banking trojan and focused on targets in the U.S., U.K., and Canada, in addition to new targets in France and Russia.

Source: <http://news.softpedia.com/news/Amount-of-New-Malware-Strains-More-than-Doubled-in-Second-Half-of-2014-481773.shtml>

22. *May 20, SC Magazine* – (International) **DDoS attacks increase and methods changed in Q1 2015, report says.** Akamai released its Q1 2015 State of the Internet Report, which found that hackers are using lower bandwidth distributed denial of service (DDoS) attacks that occur more frequently and last longer, and that Simple Service Discovery Protocol (SSDP) attacks accounted for 20 percent of attack vectors. The report also found that the gaming industry was the most targeted industry, accounting for 35 percent of all attacks, and that more than 50 percent of all DDoS attacks targeted China, Germany, and the U.S.

Source: <http://www.scmagazine.com/q1-report-shows-uptick-in-low-bandwidth-ddos-attacks/article/415876/>

23. *May 20, Securityweek* – (International) **Apples fixes security bugs with first update for Watch OS.** Apple released update 1.0.1 patching 13 vulnerabilities for its Watch operating system (OS), the iOS-based operating system that runs on the Apple Watch, addressing certain components including, the Secure Transport, kernel, Foundation framework, FontParser, IOHIDFamily, and IOAcceleratorFamily. The update also addresses the factoring RSA export key (FREAK) vulnerability, which allows a man-in-the-middle (MitM) attacker to access encrypted data.

Source: <http://www.securityweek.com/apple-fixes-security-bugs-first-update-watch-os>

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>

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

Communications Sector

24. *May 20, Lewis County Chronicle* – (Washington) **CenturyLink outage affecting almost 1,200 customers in Centralia.** Phone service for approximately 1,172 CenturyLink business and residential customers in Centralia, Washington, remained down May 20 after a construction crew inadvertently cut fiber optic lines May 19. Crews worked to repair the damaged line and did not provide an estimate on the restoration of service.
Source: http://www.chronline.com/crime/article_8931401c-ff12-11e4-9364-ef93214054fc.html

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

Commercial Facilities Sector

25. *May 20, Portland Oregonian* – (Oregon) **Chimney fire damages Salishan Spa and Golf Resort roof and lodge.** A May 20 fire that broke out around the chimney of the Salishan Spa and Golf Resort in Gleneden Beach in Lincoln County caused \$150,000 to \$200,000 in damages to the building's roof and interior.
Source: http://www.oregonlive.com/pacific-northwest-news/index.ssf/2015/05/chimney_fire_damages_salishan.html#incart_river
26. *May 20, KCBS 2 Los Angeles* – (California) **2 store owners charged in \$1.3M cell phone insurance fraud scheme.** The district attorney's office in Los Angeles announced May 20 that 2 cell phone store owners in the county were charged for allegedly billing more than \$1.3 million from an insurance company after filing false insurance claims for cell phones that were reported as stolen, lost, or damaged. The pair sold the replacement cell phones provided by the insurance company for a profit.
Source: <http://losangeles.cbslocal.com/2015/05/20/2-store-owners-charged-in-1-3m-cell-phone-insurance-fraud-scheme/>

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

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

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 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.