



Homeland
Security

Daily Open Source Infrastructure Report

14 October 2015

Top Stories

- Twenty-five coal units at Michigan power plants are scheduled to be shut down by 2020 due to additional restrictive environmental regulations and old age. – *Detroit Free Press* (See item [1](#))
- Southwest Airlines issued a statement October 12 that technical systems were repaired after a computer glitch caused 836 flight delays out of 3,355 flights scheduled October 11. – *NBC News; Associated Press* (See item [13](#))
- Officials reported October 9 that the operators of Maryland Health Benefit Exchange’s Web site improperly stored customer information while awarding over \$100 million in contracts without ensuring that the money would be spent properly. – *Washington Post* (See item [18](#))
- Officials released October 12 that 11 of the 17 dams that failed during recent heavy rains in South Carolina had been cited repeatedly for deficiencies by the State over several years. – *Columbia State* (See item [35](#))

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. *October 10, Detroit Free Press* – (Michigan) **25 Michigan coal plants are set to retire by 2020.** Additional restrictive environmental regulations and old age prompted the closure of 25 coal units at Michigan power plants, which are scheduled to be shut down by 2020. Michigan officials were ordered to submit a detailed plan in September 2016 on how the State will come into compliance with the Clean Power Plan.
Source: <http://www.freep.com/story/money/business/michigan/2015/10/10/25-michigan-coal-plants-set-retire-2020/73335550/>
2. *October 10, Associated Press* – (North Dakota) **33,000 gallons of saltwater spills.** The North Dakota Department of Health announced October 10 that 33,000 gallons of saltwater spilled from a Hillstone Environmental Partners LLC-operated site in McKenzie County. Officials reported that the spill did not impact surface waters, and the cause remains under investigation.
Source: http://bismarcktribune.com/bakken/gallons-of-saltwater-spills/article_dfe22daf-fdcd-503e-858b-f31744cb0d04.html
3. *October 10, Seattle Times* – (Washington) **Thousands without power as rain and wind topple trees.** Utility crews worked to restore power to approximately 60,000 customers in Seattle who lost service October 10 due to strong winds and several inches of rainfall.
Source: <http://www.seattletimes.com/seattle-news/weather/thousands-without-power-as-rain-and-wind-topple-trees/>

For another story, see item [26](#)

Chemical Industry Sector

4. *October 12, Reuters* – (Texas) **Partial settlement reached in deadly Texas fertilizer plant explosion.** Texas-based Adair Grain Inc., reached a partial settlement October 11 for at least 7 lawsuits claiming the company neglected plant employees after a 2013 explosion at its West Fertilizer Co facility damaged a section of the city, killed 15 people, and caused an estimated \$100,000 in damages.
Source: <http://www.reuters.com/article/2015/10/12/usa-texas-settlement-idUSL1N12C0QA20151012>

Nuclear Reactors, Materials, and Waste Sector

5. *October 13, Boston Globe* – (Massachusetts) **Pilgrim nuclear power plant to close in Plymouth.** Louisiana-based Entergy Corp., reported October 13 that its Pilgrim Nuclear Power Station in Plymouth will shut down no later than June 2019 after market conditions and increased costs led to the plant's closure, a month after the U.S. Federal Nuclear Regulatory Commission decision to downgrade the plant's safety rating.
Source: <http://www.bostonglobe.com/metro/2015/10/13/entergy-close-pilgrim-nuclear-power-station-nuclear-power-plant-that-opened/fNeR4RT1BowMrFApb7DqQO/story.html>

For another story, see item [26](#)

Critical Manufacturing Sector

See item [26](#)

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

6. *October 12, Securityweek* – (National) **Dow Jones suffers data breach.** Dow Jones & Company alerted customers October 9 after discovering that hackers targeted contact details of current and former subscribers between August 2012 – July 2015, and may have accessed financial information belonging to 3,500 individuals. There is reportedly no direct evidence that any information was stolen or misused, and law enforcement officials believe that the attack was linked to a broader hacking campaign.
Source: <http://www.securityweek.com/dow-jones-suffers-data-breach>
7. *October 9, Washington Post* – (National) **E-Trade notifies 31,000 customers that their contact info may have been breached in 2013 hack.** E-Trade notified about 31,000 customers in the week of October 5 that their personal information including email account names and physical names and addresses may have been compromised in a 2013 cyberattack. The company reportedly warned customers out of an abundance of caution and found no fraud or losses resulting from the incident.
Source: <https://www.washingtonpost.com/news/the-switch/wp/2015/10/09/e-trade-notifies-31000-customers-that-their-contact-info-may-have-been-breached-in-2013-hack/>

Transportation Systems Sector

8. *October 13, Associated Press* – (New Hampshire) **Crash cause shutdown of Interstate 93 north in Windham, no major injuries reported.** Interstate 93 north in Windham was shut down for over 2 hours October 13 while crews worked to clear the scene of an accident that involved a semi-truck and a vehicle, injuring 2 people.
Source:
<http://www.dailyjournal.net/view/story/18d7c76e49354518a7527ea54bb03db3/NH--I-93-Accident>
9. *October 13, WLKY 32 Louisville* – (Kentucky) **I-64 back open after deadly crash.** All lanes of Interstate 64 near Cannons Lane in Louisville reopened October 13 after being shut down for several hours while crews responded to a fiery single-vehicle accident that killed 1 person.
Source: <http://www.wlky.com/news/interstate-64-shutdown-in-both-directions-for-accident/35810428>

10. *October 13, Orlando Sentinel* – (Florida) **FedEx semi-truck overturns, spills packages on I-4.** The westbound lanes of Central Florida Parkway remains closed while Interstate 4 east in Orlando reopened October 13 after being shut down when a FedEx truck driver lost control and collided with another vehicle and overturned, spilling packages onto the roadway October 12. FedEx is contacting customers to inform them of the spill while workers clear the scene.
Source: <http://www.orlandosentinel.com/news/breaking-news/os-fedex-semi-crash-spilled-packages-20151013-story.html>
11. *October 13, WSPA 7 Spartanburg* – (South Carolina) **I-95 lanes are reopened after flood.** The South Carolina Department of Transportation reopened the north and south bound lanes of Interstate 95 October 13 after being shut down since the week of October 5 due to historic flooding.
Source: <http://wspa.com/2015/10/12/i-95-southbound-now-open-northbound-still-shutdown-after-flood/>
12. *October 12, USA Today* – (New York) **Burning credit card reader forces emergency landing.** Alaska Airlines Flight 17 headed to Seattle from Newark made an emergency landing in Buffalo, New York, after a credit card device began smoking from the battery compartment October 12. The plane landed safely and 181 passengers were re-booked onto another flight while the plane was inspected.
Source: <http://www.usatoday.com/story/travel/flights/todayinthesky/2015/10/12/alaska-airlines-emergency-landing/73827256/>
13. *October 12, NBC News; Associated Press* – (National) **Outdated technology likely culprit in Southwest Airlines outage.** Southwest Airlines issued a statement October 12 that technical systems were repaired after a computer glitch prevented passengers from checking in and caused 836 delays out of 3,355 flights scheduled October 11. The cause of the failure is believed to be from outdated technology.
Source: <http://www.nbcnews.com/business/travel/outdated-technology-likely-culprit-southwest-airlines-outage-n443176>

Food and Agriculture Sector

14. *October 10, U.S. Food and Agriculture* – (National) **Skipanon Brand Seafoods LLC recalls all seafood canned products because of possible health risk.** Warrenton, Oregon-based Skipanon Brand Seafoods LLC issued a voluntary recall October 9 of all lots and sizes of its Skipanon brand seafoods canned products after a Federal inspection revealed a lack of documentation and possible under-processed products that may include clostridium botulinum. The products were distributed to wholesalers and retailers in several States, and through Internet sales nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm466521.htm>

For another story, see item [4](#)

Water and Wastewater Systems Sector

15. *October 12, Bremerton Kitsap Sun* – (Washington) **Sewer spill triggers no-contact order in Port Ludlow.** A no-contact advisory has been issued for Port Ludlow Bay October 12 after 25,000 gallons of sewage spilled into the waterway due to an electrical failure at the Port Ludlow Wastewater Treatment Plant October 9 through October 10. Source: http://www.kitsapsun.com/news/local-news/sewer-spill-triggers-nocontact-order-in-port-ludlow_78002810
16. *October 8, WIS 10 Columbia* – (South Carolina) **City of Columbia announces partial repeal of system-wide boil water advisory.** City officials reported that customers in the Town of Chapin and nearby areas are no longer under a boil water advisory October 8 while all other costumers in Columbia remain under advisory while water is collected and tested following an intense flushing of the distribution system. City officials urge that citizens remain minimizing water until further notice. Source: <http://www.wistv.com/story/30210794/city-of-columbia-announces-partial-repeal-of-system-wide-boil-water-advisory>

Healthcare and Public Health Sector

17. *October 10, U.S. Food and Drug Administration* – (International) **Cook Medical expands global recall of select sizes of Beacon Tip Angiographic Catheters.** The U.S. Food and Drug Administration reported October 9 that Cook Medical expanded its October 7 recall for several lots of select sizes of its Beacon Tip Angiographic Catheters to include all lots of select sizes after the devices were found to exhibit tip splitting or separation, which has resulted in 42 Medical Device Reports. Source: <http://www.fda.gov/Safety/Recalls/ucm466545.htm>
18. *October 9, Washington Post* – (Maryland) **Audit: Maryland health-insurance site failed to protect patient information.** The Maryland Office of Legislative Audits released a report October 9 which found that the operators of Maryland Health Benefit Exchange’s Web site improperly stored Social Security numbers and other customer information, while awarding over \$100 million in contracts without ensuring that the money was being properly spent. The exchange stated that it took steps to increase security measures and safeguards to help protect consumer information. Source: https://www.washingtonpost.com/local/dc-politics/audit-maryland-health-insurance-site-failed-to-protect-patient-information/2015/10/09/68f70a14-6e9f-11e5-9bfe-e59f5e244f92_story.html

For another story, see item [26](#)

Government Facilities Sector

19. *October 12, KBZK 7 Bozeman* – (Montana) **Crews making headway on Cottonwood Gulch fire.** Crews reached 15 percent containment October 12 of the 8,300-acre Cottonwood Gulch Fire burning north of Logan in Gallatin County. Authorities are investigating the fire, which is believed to be accidental and human-caused.

Source: <http://www.kbzk.com/story/30243805/crews-making-headway-on-cottonwood-gulch-fire>

20. *October 12, Sierra Vista Herald* – (Arizona) **Bomb threat clears courthouse.** A bomb threat forced the evacuation of the Cochise County Superior Courthouse and nearby buildings in Bisbee for approximately 3 hours October 12 while police searched the structure and cleared the scene.

Source: http://www.douglasdispatch.com/news/update-bomb-threat-clears-courthouse/article_d1db981e-7134-11e5-8967-6f03f19cebad.html

21. *October 11, KTVB 7 Boise* – (Idaho) **Idaho wildfire destroys 4 structures, forces evacuations.** Fire crews worked to contain the 3,000-acre wildfire burning in the Grimes Creek area of Idaho after 4 structures were destroyed and dozens of homes in the Macks Creek and Pine Creek areas were under evacuation orders October 11

Source: <http://www.king5.com/story/news/local/wildfires/2015/10/11/idaho-wildfire-destroys-4-structures-forces-evacuations/73785276/>

Emergency Services Sector

22. *October 12, KOMU 8 Columbia* – (Missouri) **911 service restored in east Columbia.** Emergency 9-1-1 service for more than 7,500 Joint Communications customers in Boone County was restored October 12 after CenturyLink crews resolved issues due to an isolated incident that knocked out services October 11.

Source: <http://www.komu.com/news/911-service-restored-in-east-columbia/>

Information Technology Sector

23. *October 13, Securityweek* – (International) **Cisco IOS rootkits can be created with limited resources: Researchers.** Security researchers from Grid32 released research revealing that cybercriminals could easily create a basic Cisco IOS rootkit within a month or less which could rival the effectiveness of the SYNful Knock malware designed to replace router firmware. Cisco has implemented several new security technologies in current devices to help mitigate threats.

Source: <http://www.securityweek.com/cisco-ios-rootkits-can-be-created-limited-resources-researchers>

24. *October 12, Securityweek* – (International) **Command injection flaw found in HP SiteScope.** Security researchers from Rapid7 and Knowledge Consulting Group discovered a vulnerability in HP SiteScope in which an attacker with local system access could execute arbitrary operating system (OS) commands by accessing a default deployment of the product's administration panel.

Source: <http://www.securityweek.com/command-injection-flaw-found-hp-sitescope>

25. *October 12, Help Net Security* – (International) **Thousands of Zhone SOHO routers can easily be hijacked.** A security researcher from Vantage Point Security revealed a number of recently patched vulnerabilities, including a remote code execution (RCE) flaw in Zhone Technologies Small Office/Home Office (SOHO) routers, and reported

that some users could not access the products' administration panels to apply the corresponding firmware update.

Source: <http://www.net-security.org/secworld.php?id=18967>

26. *October 12, Securityweek* – (International) **Schneider Electric patches flaw in Motion USA website.** Schneider Electric patched a cross-site scripting (XSS) vulnerability on its e-order.biz Web site which allowed customers to order products from Schneider Electric Motion USA. The vulnerability could allow an attacker to execute JavaScript code to steal cookies and session identifiers to hijack accounts or redirect users to phishing sites due to the site's failure to sanitize the input passed by remote users in a hypertext transfer protocol (HTTP) request.

Source: <http://www.securityweek.com/schneider-electric-patches-flaw-motion-usa-website>

27. *October 11, Softpedia* – (International) **Kaspersky Antivirus fixes bug that allowed attackers to block Windows Update and other services.** Kaspersky Antivirus fixed a flaw in its Internet Security package's Network Attack Blocker component that could have allowed an attacker to spoof traffic and to use the product to block services such as Microsoft Windows Update, Kaspersky's update servers, or other services that would enable a system to be compromised further. The company reported that the flaw had never been exploited in the wild.

Source: <http://news.softpedia.com/news/vulnerability-open-to-abuse-fixed-in-kaspersky-internet-security-antivirus-494280.shtml>

28. *October 11, Softpedia* – (International) **Android Adware hits to Google Play Store once again.** Google removed applications from the Google Play Store after security researchers from ESET discovered a new Android adware in which the "Cheats for Pou," "Cheats for Subway," and "Guide for SubWay," applications were compromised with malware that would show fullscreen ads intermittently.

Source: <http://news.softpedia.com/news/android-adware-hits-to-google-play-store-once-again-494285.shtml>

29. *October 10, Softpedia* – (International) **DDoS attacks can bypass mitigation services by taking aim at a website's origin IP.** Security researchers from the U.S. and Belgium released research revealing that most Cloud-Based Security Providers' (CBSP) distributed denial-of-service (DDoS) mitigation can be bypassed by attackers who discover targeted Web site's origin Internet protocol (IP) addresses either by analyzing outbound connections, Secure Sockets Layer (SSL) certificates, via sensitive files hosted on the server, or during migration or maintenance operations that expose the site. Researchers found that 71.5 percent of 17,877 scanned Web sites revealed origin IP addresses.

Source: <http://news.softpedia.com/news/ddos-attacks-can-bypass-mitigation-services-by-taking-aim-at-a-website-s-origin-ip-494273.shtml>

For additional stories, see items [6](#) and [32](#)

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>

Communications Sector

Nothing to report

Commercial Facilities Sector

30. *October 12, Tallahassee Democrat* – (Florida) **Fire prompts evacuation of Courtyard Marriott.** Tallahassee fire crews reported October 12 that the Courtyard Marriott sustained an estimated \$250,000 in damages after a fire began on the outside of the building and spread into the attic. Residents were evacuated from the first two floors and no injuries were reported.
Source: <http://www.tallahassee.com/story/news/2015/10/12/courtyard-marriott-evacuated-fire/73840882/>
31. *October 12, Pleasanton Patch; Bay City News* – (California) **Bomb threat prompts evacuation of Pleasanton Home Depot.** The Pleasanton Square Shopping Center, housing several stores including a Home Depot, were evacuated for about 2 hours October 11 while police crews searched for a suspicious item after a Home Depot employee allegedly received a bomb threat via phone. Bomb crews responded to the call and found no explosive device.
Source: <http://patch.com/california/pleasanton/bomb-threat-prompts-evacuation-pleasanton-home-depot-0>
32. *October 12, AL.com* – (International) **America's thrift store hit by cyber attack, Birmingham-based company says credit card data exposed.** Birmingham-based America's Thrift Store reported October 12 that cyber criminals from Eastern Europe accessed its systems through a third-party provider and installed malwares onto its system, allowing unauthorized access to customers' payment card numbers from September 1 – September 27. Officials reported the malware has since been removed and the U.S. Secret Service is investigating the breach.
Source:
http://www.al.com/news/index.ssf/2015/10/americas_thrift_store_hit_by_c.html
33. *October 11, KWTX 10 Waco* – (Texas) **Area carnival evacuated after juvenile mob fights, riots.** The Wright Amusement Carnival in College Station was evacuated October 11 after 4 uniformed off-duty officers, working as security guards, tried to contain a parking lot fight and were met with aggressive actions, prompting the officers to call for police assistance after a mob of nearly 1,000 juveniles crowded the off-duty officers. Two officers were injured and 5 people were arrested.
Source: <http://www.kwtx.com/home/headlines/Area-Carnival-Evacuated-After->

[Juvenile-Mob-Fights-Riots-331929531.html](http://www.wset.com/news/local/appomattox-walmart-evacuated-following-bomb-threat)

34. *October 10, WSET 13 Lynchburg* – (Virginia) **Appomattox Walmart evacuated following bomb threat.** Officials reported that a Walmart in Appomattox reopened October 10 after a bomb threat prompted the evacuation of employees and shoppers for nearly 4 hours while State police searched the entire building. No devices were found and no injuries were reported.
Source: <http://wset.com/news/local/appomattox-walmart-evacuated-following-bomb-threat>

Dams Sector

35. *October 13, Columbia State* – (South Carolina) **Failed Richland dams had flaws, inspection records show.** South Carolina officials released records October 12 that 11 of the 17 dams that failed in Richland County following historic rains throughout the month of October, were cited repeatedly over several years in State inspection reports according to South Carolina Department of Health and Environmental Control. Officials also reported that they had no record for two of the dams that breached and two others were not under the agency's jurisdiction.
Source: <http://www.thestate.com/news/local/article38896089.html>



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.