



Homeland
Security

Daily Open Source Infrastructure Report

25 November 2014

Top Stories

- XPLORE Energy SPV-1, Inc., agreed to pay a \$3.1 million fine and serve a 3-year probation term after pleading guilty to knowingly violating the Clean Water Act by discharging oily wastewater into the Breton Sound and the Gulf of Mexico off Louisiana. – *Associated Press* (See item [1](#))
- A tour bus traveling from Los Angeles to Pasco, Washington, crashed in northern California November 23 killing 1 passenger and injuring 28 others when the bus drifted off Interstate 5 and overturned into an embankment. – *Los Angeles Times* (See item [4](#))
- Symantec researchers reported the discovery of a piece of sophisticated cyber espionage malware that works as a backdoor to steal information from compromised systems and appears to have been created by a nation-state actor. – *Securityweek* (See item [21](#))
- The former general manager of the Sleep Inn hotel in Allendale, Michigan, was charged November 21 for allegedly stealing more than \$872,929 by directing credit card payments to personal accounts. – *Grand Rapids Press* (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. *November 21, Associated Press* – (Louisiana) **XPLOR Energy pleads to Clean Water Act Violation.** XPLOR Energy SPV-1, Inc., an Oklahoma-based oil company agreed to pay a \$3.1 million fine and serve a 3-year probation term after pleading guilty for knowingly violating the federal Clean Water Act by discharging oily wastewater into the Breton Sound and the Gulf of Mexico from an offshore facility off Louisiana. Source: <http://www.washingtontimes.com/news/2014/nov/21/xplor-energy-pleads-to-clean-water-act-violation/>

For another story, see item [21](#)

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

Chemical Industry Sector

Nothing to report

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

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

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

Critical Manufacturing Sector

Nothing to report

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

Defense Industrial Base Sector

Nothing to report

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

Financial Services Sector

2. *November 24, Securityweek* – (International) **Fraud service uses charity websites to validate stolen credit card data.** Researchers with PhishLabs reported November 21 that it had found online fraudsters using a bot and an IRC channel to conduct transactions on the Web sites of charity or non-profit organizations in order to test the validity of stolen payment card information and related personal information. Source: <http://www.securityweek.com/fraud-service-uses-charity-websites-validate-stolen-credit-card-data>

3. *November 21, U.S. Securities and Exchange Commission* – (New York) **SEC charges CEO and close friend with insider trading ahead of company sale.** Two New York City men, including one who served as CEO and a member of the board directors for GenTek Inc., agreed to pay a total of \$324,000 to resolve U.S. Securities and Exchange Commission charges that the former CEO passed on nonpublic information to the second man, who used it to engage in insider trading and make \$164,260 in illicit profits ahead of GenTek's sale to American Securities.
Source: <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543516329>

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

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

Transportation Systems Sector

4. *November 23, Los Angeles Times* – (California) **One dead, dozens hurt in Northern California bus crash.** A tour bus traveling from Los Angeles to Pasco, Washington, crashed in northern California November 23 killing 1 passenger and injuring 28 others, with 11 in serious or critical conditions when the bus drifted off Interstate 5 and overturned into an embankment. The same bus was reportedly involved in an earlier minor crash at a Denny's restaurant in Red Bluff, California, but no injuries were reported.
Source: <http://www.latimes.com/local/lanow/la-me-ln-bus-crash-story.html>
5. *November 23, KPIX 5 San Francisco* – (California) **Man arrested after breaching security, commandeering a service vehicle at San Jose Airport.** Police arrested a man November 23 for allegedly commandeering an airport work truck at Mineta San Jose International Airport after he broke away from airport authorities while waiting for police to arrive when he was spotted and detained near a restricted loading ramp at the airport.
Source: <http://sanfrancisco.cbslocal.com/2014/11/23/police-capture-man-who-breached-security-mineta-san-jose-airport/>
6. *November 22, WKYC 3 Cleveland* – (Ohio) **Fire breaks out at Middleburg Heights UPS facility.** Authorities are investigating after a fire broke out at a United Postal Service Distribution Center in Middleburg Heights November 21. All employees were safely evacuated and November 22 operations were moved to a facility in Cleveland.
Source: <http://www.wkyc.com/story/news/local/cuyahoga-county/2014/11/21/ups-fire/19375003/>
7. *November 22, Detroit News* – (Michigan) **Metro Detroit roads improve, flights resume.** Icy conditions temporarily closed four parallel runways for several hours at Detroit Metropolitan Airport and a Delta Air Lines flight from Portland to Detroit skidded off a taxiway into the grass while taxiing after landing November 22 due to the icy surfaces.
Source: <http://www.detroitnews.com/story/news/local/metro-detroit/2014/11/22/ice->

[causing-havoc-metro-detroit-roads/19396847/](http://www.wsbtv.com/news/news/local/bus-hits-plane-hartsfield-jackson-airport/njC84/)

8. *November 22, WSB 2 Atlanta* – (Georgia) **Bus hits plane at Hartsfield-Jackson Airport.** Passengers onboard an American Airlines flight were evacuated off the plane and re-booked onto new flights after a bus crashed into the wing of the plane while it was parked at a gate at Hartsfield-Jackson International Airport November 21. No injuries were reported.
Source: <http://www.wsbtv.com/news/news/local/bus-hits-plane-hartsfield-jackson-airport/njC84/>

For another story, see item [21](#)

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

Food and Agriculture Sector

9. *November 24, U.S. Department of Agriculture* – (National) **Minnesota firm recalls ground beef products due to possible E. Coli O157:H7 contamination.** The Food Safety and Inspection Service announced November 22 a recall of 1,200 pounds of Ranchers Legacy Meat Co., ground beef products due to possible E. coli O157:H7 contamination. The affected products were produced November 19 and packaged in plastic cryovac sealed packets before they were shipped to distributors nationwide.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2014/recall-082-2014-release>
10. *November 23, Associated Press* – (Illinois) **Some 30 horses die in stable fire outside Chicago.** Thirty-two horses perished and a 2-story barn collapsed during a stable fire at Valley View Acres boarding facility in unincorporated Woodstock, Illinois, November 22. Authorities are investigating the source of the fire that caused more than \$1 million in damage.
Source: <http://www.aol.com/article/2014/11/23/some-30-horses-die-in-stable-fire-outside-chicago/20997869/>
11. *November 21, U.S. Food and Drug Administration* – (National) **Kozy Shack Enterprises, LLC issues allergen alert on unlabeled Foodservice Chocolate Pudding Cups.** The U.S. Food and Drug Administration reported November 21 that Kozy Shack Enterprises, LLC issued a recalled for 4 ounce containers of its Foodservice Kozy Shack Simply Well Chocolate Pudding due to undeclared milk and lack of product labeling. The affected product was distributed via foodservice distribution channels in 20 States.
Source: <http://www.fda.gov/Safety/Recalls/ucm424272.htm>

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

Water and Wastewater Systems Sector

12. *November 24, Lihue Garden Island* – (Hawaii) **Broken pump causes water outage on**

Westside. Water service was expected to be restored to about 900 residents in the Makaweli, Kaumakani, and Pakala area November 24 after a pump in a water system owned and managed by Gay & Robinson failed and disrupted service November 22. Source: http://thegardenisland.com/news/local/broken-pump-causes-water-outage-on-westside/article_6ea09ec6-7382-11e4-bec9-97768c499692.html

13. *November 23, Pittsburgh Tribune-Review* – (Pennsylvania) **Water service restored in Derry after leaks.** Most residents of west Derry were without water service for nearly 12 hours due to a water leak that occurred November 22. Source: <http://triblive.com/news/westmoreland/7224110-74/forsha-service-authority>
14. *November 21, NJ.com* – (New Jersey) **Fallout from sewer main break: don't fish off Jersey City coast, DEP says.** New Jersey's Department of Environmental Protection issued an advisory warning residents to avoid direct contact with and to refrain from fishing in the waters of the Lower Hudson River, New York Bay, and Kill Van Kull after a 54-inch high pressure sewer line ruptured November 20 and spilled untreated sewage. The advisory remains in effect until further notice, and authorities stated that some sewage would also have to be discharged in order to make repairs. Source: http://www.nj.com/hudson/index.ssf/2014/11/fallout_from_sewer_main_break_dont_fish_off_jersey_city_coast_dep_says.html

For another story, see item [1](#)

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

Healthcare and Public Health Sector

15. *November 21, Boston Globe* – (Massachusetts) **Beth Israel fined \$100,000 for patient data breach.** A settlement between Beth Israel Deaconess Medical Center and the Massachusetts's attorney general's office was reached November 21 to settle claims that the medical center's lax data security led to the theft of a physician's unattended and unencrypted laptop in May 2012 which housed the personal and health information of 3,796 patients and Beth Israel employees. The medical center will pay \$100,000 to settle the complaint. Source: <http://www.bostonglobe.com/business/2014/11/21/beth-israel-fined-for-patient-data-breach/W8LT4a0gN6NMT93KtEDq7H/story.html>

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

Government Facilities Sector

16. *November 24, WEWS 5 Cleveland* – (Ohio) **Anonymous claims responsibility for taking down Cleveland's website after shooting.** The City of Cleveland confirmed November 24 that its official Web site was down due to a cyber attack. Attackers claiming affiliation with the Anonymous hacktivist claimed responsibility for the attack in a video and social media message referencing a Cleveland Police-involved shooting.

Source: <http://www.newsnet5.com/news/local-news/cleveland-metro/anonymous-claims-responsibility-for-taking-down-clevelands-website-after-tamir-rice-shooting>

17. *November 23, Green Bay Press-Gazette* – (Wisconsin) **Hundreds, including UWGB, lose power.** University of Wisconsin-Green Bay officials closed academic buildings, a library, computer labs, events center, and the University Union due to a power outage prompted by a failure in an electrical transformer November 23. Crews worked to restore service prior to the start of classes November 24.

Source:

<http://www.greenbaypressgazette.com/story/news/local/2014/11/23/transformer-problem-knocks-power-much-uwgb/19466605/>

18. *November 23, KABB 29 San Antonio* – (Texas) **All-clear sounded at Fort Sam Houston, suspect in custody.** Officials reported November 23 that a suspect was in custody following the lockdown of Fort Sam Houston and the San Antonio Military Medical Center in Texas that lasted more than 3 hours due to a suspicious vehicle.

Source: <http://www.foxsanantonio.com/news/features/top-stories/stories/-allclear-sounded-at-fort-sam-houston-suspect-custody-8363.shtml>

19. *November 21, WSIL 3 Harrisburg* – (Illinois) **Bomb threat closes 2 courthouses.** A suspect was in police custody in connection to a bomb threat called in to Johnson County 9-1-1 which prompted the evacuation and closure of the White County and Saline County courthouses in Illinois November 21.

Source: <http://www.wsilv.com/news/local/Bomb-Threat-Closes-2-Courthouses--283482661.html>

20. *November 21, Green Bay Press-Gazette* – (Wisconsin) **De Pere City Hall evacuated for CO leak.** De Pere City Hall in Wisconsin was evacuated for more than 2 hours November 21 while firefighters shut off boilers and ventilated the building following a carbon monoxide leak. Crews worked to repair the malfunctioning boiler while a second unaffected boiler restored heat to the building.

Source: <http://www.greenbaypressgazette.com/story/news/local/2014/11/21/de-pere-city-hall-evacuated-co-leak/19353187/>

For another story, see item [21](#)

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

Emergency Services Sector

Nothing to report

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

Information Technology Sector

21. *November 24, Securityweek* – (International) **Symantec uncovers stealthy nation-**

state cyber attack platform. Symantec researchers reported the discovery of a piece of sophisticated cyber espionage malware dubbed Regin that works as a backdoor to steal information from compromised systems and appears to have been created by a nation-state actor. The malware is modular in design and has predominantly targeted small businesses, individuals, and telecoms companies, as well as the hospitality, energy, and airline industries and research organizations.

Source: <http://www.securityweek.com/symantec-uncovers-stealthy-nation-state-cyber-attack-platform>

22. *November 24, The Register* – (International) **Sony quietly POODLE-proofs**

Playstations. Sony released a patch for its Playstation 3 and Playstation 4 gaming consoles that adds Transport Layer Security to the consoles' apps and browsers and removes the use of SSL 3.0 to protect against POODLE attacks.

Source:

http://www.theregister.co.uk/2014/11/24/sony_playstation_update_spells_death_knell_for_poodle/

23. *November 21, Softpedia* – (International) **Facebook bug remains unpatched, risk is**

partially mitigated. A researcher who reported a flaw in Facebook that could allow posting to a user's timeline without permission in 2013 reported that the proof-of-concept for the attack still works in some cases where certain third-party Facebook apps do not implement the new content share model Facebook developed to address the issue.

Source: <http://news.softpedia.com/news/Facebook-Bug-Remains-Unpatched-Risk-Is-Partially-Mitigated-465611.shtml>

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

See item [21](#)

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

Commercial Facilities Sector

24. *November 24, WAVY 10 Portsmouth* – (Virginia) **Over 60 displaced after downtown Suffolk apartment fire.** About 60 residents were temporarily displaced from the Suffolk Towers apartment complex in Virginia November 23 due to a fire that started in an electrical room and filled the building with heavy smoke.

Source: <http://wavy.com/2014/11/23/downtown-apartment-fire-closes-roads-in-suffolk/>

25. *November 24, Marietta Daily Journal* – (Georgia) **Marietta apartment fire claims 16 units.** A November 22 fire at The Walton at Columns Drive apartment complex in Marietta, Georgia, destroyed or damaged more than 16 units and displaced several residents.

Source: http://mdjonline.com/view/full_story/26145843/article-Marietta-apartment-fire-claims-16-units

26. *November 24, WUSA 9 Washington, D.C.* – (Virginia) **Workers with torches caused Sears Auto Center fire, say officials.** Approximately 100 customers and staff were evacuated from a Sears Auto Center store at Fair Oaks Mall in Fairfax November 23 while firefighters extinguished a fire inside a trash compactor that was sparked by workers using acetylene torches. Crews worked for about 2 hours to ventilate the building, and one person was treated at the scene for minor injuries.

Source: <http://www.wusa9.com/story/news/2014/11/24/sears-auto-center-fire-fairfax-county-fair-oaks-mall-va/19477607/>

27. *November 24, Baton Rouge Advocate* – (Louisiana) **Baton Rouge firefighters battle tire warehouse blaze for 12 hours.** Firefighters spent about 12 hours November 22 – November 23 battling a fire at a Baton Rouge warehouse that was filled with tires and heavy machinery. The metal structure collapsed as a result of the blaze and damages were estimated at more than \$1 million.

Source: <http://theadvocate.com/news/10917734-123/baton-rouge-firefighters-battle-tire>

28. *November 22, Palm Beach Post* – (Florida) **Bomb threat clears CityPlace Publix in West Palm; no explosives found.** A Publix Super Market at CityPlace in West Palm Beach was evacuated for more than 2 hours November 22 while authorities investigated a phoned bomb threat. The store reopened after police cleared the scene.

Source: <http://www.palmbeachpost.com/news/news/local/bomb-threat-clears-cityplace-publix-in-west-palm-n/njDKR/>

29. *November 22, Grand Rapids Press* – (Michigan) **Hotel general manager accused of stealing nearly \$900,000 in credit card scheme.** The former general manager of the Sleep Inn hotel in Allendale was charged with wire fraud and money laundering according to an indictment unsealed November 21 for allegedly stealing more than \$872,929 by directing credit card payments to personal accounts through the form of fraudulent customer refunds between October 2006 and April 2013.

Source: http://www.mlive.com/news/grand-rapids/index.ssf/2014/11/hotel_general_manager_accused.html

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

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

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.