



## Daily Open Source Infrastructure Report 01 February 2016

### Top Stories

- San Diego officials announced indictments against attorneys and medical professionals January 28 for their roles in a workers' compensation fraud scheme, which resulted in millions of dollars' worth of fraudulent claims. – *KSWB 69 San Diego* (See item [9](#))
- As many as 179 students and staff members became ill January 28 due to a carbon monoxide leak at Marshall Middle School in Texas, which prompted the school's evacuation and closure. – *KPRC 2 Houston* (See item [11](#))
- A January 28 report on the Washington, D.C. Metropolitan Police Department's use of excessive force found no evidence that the department has an excessive force problem and that intentional discharges of weapons have declined. – *Washington Post* (See item [17](#))
- Federal authorities reported January 28 that a man was charged for providing support to a terrorist group after he allegedly released the personal information of more than 1,000 U.S. soldiers and government employees to the group. – *The Register* (See item [22](#))

---

### 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

Nothing to report

## Chemical Industry Sector

Nothing to report

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

## Critical Manufacturing Sector

1. *January 28, U.S. Department of Labor* – (Alabama) **OSHA cites auto parts manufacturer for willfully exposing workers to amputations, other hazards at Alabama facility.** The Occupational Safety and Health Administration cited Daeil USA Corp., for 1 willful, 5 repeated, 10 serious, and 1 other-than-serious safety violations January 28 after a Federal investigation at the Valley, Alabama facility revealed that the company willfully failed to develop, document, and utilize specific procedures to prevent multiple types of machinery from starting during maintenance and servicing, exposed workers to slipping hazards from wet floors, and did not provide an eyewash station for workers that handled corrosive materials, among other violations. Proposed penalties total \$171,870.

Source:

[https://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=29490](https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=29490)

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

Nothing to report

## Transportation Systems Sector

2. *January 29, WPLG 10 Miami* – (Florida) **Tri-Rail delays still expected after train derails in Pompano Beach.** A Tri-Rail train derailed January 28 in Pompano Beach causing an engine to catch fire and spill 2,200 gallons of diesel fuel onto the track. Riders were evacuated and transported between stations via buses while authorities investigated the cause of the derailment.  
Source: <http://www.local10.com/news/tri-rail-train-derails-in-pompano-beach>
3. *January 28, San Diego Union-Tribune* – (California) **Truck plummets off freeway in fiery crash.** Several lanes of northbound Interstate 805 in Kearny Mesa were closed for

hours January 28 after a box truck was rear-ended by another vehicle and flipped over a State Route 163 railing, crashing onto north Interstate 805 below before bursting into flames. Four people suffered minor injuries.

Source: <http://www.sandiegouniontribune.com/news/2016/jan/28/truck-plummets-off-freeway-in-fiery-crash/>

4. *January 28, LancasterOnline* – (Pennsylvania) **Crash closes Route 30 east of Gap.** A multi-vehicle accident closed a portion of Route 30 in Lancaster, Pennsylvania, for 3 hours January 28 while emergency personnel responded.

Source: [http://lancasteronline.com/news/local/wreck-along-lincoln-highway-closes-traffic-thursday-afternoon/article\\_92241c68-c5f4-11e5-add4-e7f3c63f4cc9.html](http://lancasteronline.com/news/local/wreck-along-lincoln-highway-closes-traffic-thursday-afternoon/article_92241c68-c5f4-11e5-add4-e7f3c63f4cc9.html)

## **Food and Agriculture Sector**

5. *January 29, Associated Press* – (National) **More illnesses in listeria outbreak in Dole packaged salads.** The U.S. Centers for Disease Control and Prevention announced January 29 that three additional people in Connecticut, Missouri, and New York were reportedly sickened as a result of a Listeria outbreak linked to packaged salads made at the Ohio-based Dole processing facility. The outbreak has caused 1 death and 15 hospitalizations across 8 States since July 2015.

Source: <http://wgntv.com/2016/01/29/more-illnesses-in-listeria-outbreak-in-dole-packaged-salads/>

## **Water and Wastewater Systems Sector**

6. *January 28, Fayetteville Observer* – (North Carolina) **Lillington under boil water advisory; city's tank is fine.** Officials issued a boil water advisory for customers in the town of Lillington through January 28 after a January 27 leak in one of the city's main water lines led to a loss in water pressure to about half the city. Crews repaired the line and restored water pressure.

Source: [http://www.fayobserver.com/news/local/harnett-county-under-a-boil-water-advisory/article\\_adc84a39-6c6e-53b8-a2a5-ba0dc4028711.html](http://www.fayobserver.com/news/local/harnett-county-under-a-boil-water-advisory/article_adc84a39-6c6e-53b8-a2a5-ba0dc4028711.html)

7. *January 27, Sheboygan Press; USA Today* – (Michigan) **224K gallons of sewage leaked into Lake Michigan.** Sheboygan officials announced January 27 that an estimated 224,000 gallons of sewage leaked into Lake Michigan the week of January 18 due to a cracked pipe. Crews installed a temporary fix January 23 until a permanent fix for the pipe can be installed.

Source: <http://www.sheboyganpress.com/story/news/local/2016/01/26/city-224k-gallons-sewage-leaked-into-lake/79368782/>

## **Healthcare and Public Health Sector**

8. *January 29, Berkshire Eagle* – (Massachusetts) **Berkshire Health Systems plagued by malware; patient, payment data safe.** Massachusetts-based Berkshire Health Systems announced January 28 that its systems were impacted by malware during the week of January 25, but that no patient health or payment information was compromised. The

health system responded immediately upon discovery of the malware and continues to work to ensure all systems are restored to normal operations.

Source: [http://www.berkshireagle.com/local/ci\\_29445753/berkshire-health-systems-plagued-by-malware-patient-payment](http://www.berkshireagle.com/local/ci_29445753/berkshire-health-systems-plagued-by-malware-patient-payment)

9. *January 28, KSWB 69 San Diego* – (California) **13 indicted in huge health care fraud case.** The San Diego County District Attorney’s Office announced 13 indictments against attorneys and medical professionals January 28 for their roles in a workers’ compensation fraud scheme in which they allegedly paid \$450,000 in kickback payments to owners and operators of chiropractic clinics in San Diego, Escondido, and Calexico in exchange for patient referrals, resulting in millions of dollars in fraudulent workers’ compensation insurance claims. Charges were also announced against three patient recruiters and four corporations for allegedly recruiting people to file workers’ compensation claims for on-the-job injuries and directing patients to specific chiropractors involved in the scheme.  
Source: <http://fox5sandiego.com/2016/01/28/13-indicted-in-huge-health-care-fraud-case/>
10. *January 28, California Department of Public Health* – (California) **California Department of Public Health issues penalties to 8 hospitals.** Eight hospitals were penalized by the California Department of Public Health January 28 following investigations which found that the facilities’ noncompliance with licensing requirements caused, or could potentially cause serious injury or death to patients. Fines totaled \$483,650.  
Source: <https://www.cdph.ca.gov/Pages/NR16-004.aspx>

## Government Facilities Sector

11. *January 29, KPRC 2 Houston* – (Texas) **Dozens of students hospitalized after carbon-monoxide leak at Beaumont middle school.** As many as 179 students and staff members became ill January 28 due to a carbon monoxide leak at Marshall Middle School in Beaumont, Texas, which prompted the school’s evacuation. The school will remain closed January 29 while authorities investigate the source of the leak.  
Source: <http://www.click2houston.com/news/students-hospitalized-after-carbon-monoxide-leak-at-middle-school-in-beaumont>
12. *January 29, Associated Press* – (International) **Navy commander pleads guilty in bribery case, faces up to 20 years in prison.** A U.S. Navy commander pleaded guilty January 28 to charges connected to his role in helping divert ships to Asian ports by providing Singapore-based Glenn Defense Marine Asia, Ltd., with classified information from 2011 – 2012 in exchange for kickbacks and bribes. The scheme led the contractor to overbill the Navy by at least \$20 million.  
Source: <http://www.foxnews.com/us/2016/01/29/navy-commander-pleads-guilty-in-bribery-case-faces-up-to-20-years-in-prison.html>
13. *January 29, WHDH 7 Boston* – (Massachusetts) **13 students suffer minor injuries in Framingham school bus crash.** A driver and 13 students from Dunning and

Hemingway schools were transported to area hospitals with injuries following an accident involving a school bus and another vehicle at an intersection in Framingham January 27.

Source: <http://www.whdh.com/story/31083866/accident-involving-school-bus-in-framingham-13-students-injured>

14. *January 29, Associated Press* – (Ohio) **Ohio EPA: Unacceptable lead levels in school drinking water.** T.C. Gurney Elementary School in Chagrin Falls announced January 29 that it will provide bottled drinking water and will shut off drinking fountains after the Ohio Environmental Protection Agency found unacceptable levels of lead in the school's drinking water. Health officials are continuing to monitor levels.

Source: <http://www.wral.com/ohio-epa-unacceptable-lead-levels-in-school-drinking-water/15291368/>

15. *January 28, WAFF 48 Huntsville* – (Alabama) **6 transported to hospital after carbon monoxide leak at Guntersville State Park Lodge.** A carbon monoxide leak due to malfunctioning exhaust fans on boilers forced the evacuation of more than 100 people from a Lake Guntersville State Park lodge in Alabama after 6 people became sick and were transported to local hospitals January 28. Authorities are investigating the incident.

Source: <http://www.wbrc.com/story/31083634/6-transported-to-hospital-after-carbon-monoxide-leak-at-guntersville-state-park-lodge>

For another story, see item [22](#)

## **Emergency Services Sector**

16. *January 28, CBS News; Associated Press* – (California) **Calif. prison teacher arrested, allegedly helped 3 inmates escape.** Officials arrested a Rancho Santiago Community College District employee who taught English as a second language at the Orange County Central Men's Jail January 28 for her alleged involvement in helping three inmates escape from the jail January 22. The three inmates remain at large.  
Source: <http://www.cbsnews.com/news/california-prison-teacher-arrested-for-allegedly-helping-3-inmates-escape/>
17. *January 28, Washington Post* – (Washington, D.C.) **Excessive force not a problem in the D.C. police force, but issues remain.** A Washington, D.C. auditor commissioned report on the Metropolitan Police Department's use of excessive force and shootings by officers was released January 28 reporting that researchers found no evidence that the police force has an excessive-use-of-force problem, that intentional discharges of weapons have declined, and that the number of fatal shootings by police has remained relatively constant, among other findings. The review also found several procedural and substantive shortcomings in the way some internal investigations were conducted.  
Source: [https://www.washingtonpost.com/local/public-safety/excessive-force-not-a-problem-in-the-dc-police-force-but-issues-remain/2016/01/27/a8357698-c4fd-11e5-8965-0607e0e265ce\\_story.html](https://www.washingtonpost.com/local/public-safety/excessive-force-not-a-problem-in-the-dc-police-force-but-issues-remain/2016/01/27/a8357698-c4fd-11e5-8965-0607e0e265ce_story.html)

## Information Technology Sector

18. *January 29, Help Net Security* – (International) **60+ trojanized Android games lurking on Google Play.** Researchers from Dr. Web found over 60 game apps offered on the Google Play store were embedded with the malicious Xiny trojan that can download additional malicious apps and collect device information such as the device's International Mobile Station Equipment Identity (IMEI) and International Mobile Subscriber Identity (IMSI), and send the data to a command and control (C&C) server via 30 different game developer accounts including Billapps, Conexagon Studio, and Fun Color Games, among other accounts. Researchers believe the accounts are operated by the same cybercriminals.  
Source: [http://www.net-security.org/malware\\_news.php?id=3195](http://www.net-security.org/malware_news.php?id=3195)
19. *January 29, The Register* – (International) **Two-thirds of Android users vulnerable to web history sniff ransomware.** Researchers from Symantec reported that two in three devices running Android versions prior to 5.0 (Lollipop) were susceptible to the Lockdroid ransomware, which tricks users into allowing malicious code to gain administrative privileges via overlaid popups that uses a fake message disguised from the U.S. Department of Justice to trick victims' into paying a fee to unlock their devices after the message prompts them that their devices have been locked due to visiting inappropriate Web sites. In addition, the malware is capable of changing the device personal identification number (PIN) and deleting user data through a factory reset.  
Source: [http://www.theregister.co.uk/2016/01/29/android\\_ransomware/](http://www.theregister.co.uk/2016/01/29/android_ransomware/)
20. *January 29, SecurityWeek* – (International) **Facebook pays out \$7,500 bounty for account hijacking flaw.** A researcher discovered a serious cross-site scripting (XSS) vulnerability that could allow attackers to compromise users' Facebook accounts by using several Facebook plugins designed in an iframe, which bypasses protections and can allow attackers to steal users' cross-site request forgery (CSRF) token and compromise users' accounts by convincing a user to click or visit a malicious link the hacker controls. Once the victim opens the malicious link, the hacker can execute any action to the victims' account.  
Source: <http://www.securityweek.com/facebook-pays-out-7500-bounty-account-hijacking-flaw>
21. *January 29, Help Net Security* – (International) **OpenSSL bug that could allow traffic decryption has been fixed.** The OpenSSL Project released updates to its security protection system to protect its products against the malicious Logjam, and released new versions of its OpenSSL cryptographic library including OpenSSL 1.0.2f and 1.0.1r, which patches two security flaws that could have been exploited by attackers to obtain keys to decrypt secure communication and obtain sensitive information.  
Source: <http://www.net-security.org/secworld.php?id=19389>
22. *January 28, The Register* – (International) **Alleged ISIL hacker faces US terror charges for doxing soldiers.** The U.S. Department of Justice and the FBI reported January 28 that a man was extradited from Malaysia to Virginia after being charged with hacking crimes and for providing support to a Middle Eastern terrorist group after

he allegedly released the personal information of more than 1,000 U.S. soldiers and government employees to the group who intended to use the information to attack the U.S. military and government personnel.

Source:

[http://www.theregister.co.uk/2016/01/28/alleged\\_isil\\_hacker\\_faces\\_us\\_terror\\_charges/](http://www.theregister.co.uk/2016/01/28/alleged_isil_hacker_faces_us_terror_charges/)

### **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**

See items [18](#) and [19](#)

### **Commercial Facilities Sector**

See item [22](#)

### **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.