Daily Open Source Infrastructure Report
19 February 2016

Top Stories

- Toyota Motor Corporation issued a recall February 18 for more than 2.9 million sport utility vehicles worldwide due to potentially faulty seat belts in second-row window seats. – *Associated Press* (See item **4**)
- The Massachusetts Bay Transportation Authority's Orange Line in Boston was evacuated along with two trains February 16 after a metal panel struck the electrified third rail filling the station with smoke and causing the trains to become disabled. – *Associated Press* (See item **10**)
- Officials announced February 17 that Interstate 70 in the city of Glenwood Springs in Colorado will be closed for several weeks while crews continue to remove loose rocks following a February 15 rock slide. – *Associated Press* (See item **11**)
- Federal authorities announced February 17 that it reached settlements with 51 hospitals in 15 States totaling more than $23 million for violations over the improper embedding of implantable cardioverter defibrillator devices. – *U.S. Department of Justice* (See item **17**)

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. *February 18, Associated Press* – (Louisiana) **EPA: Cleco coal-fired power plant out of compliance.** The U.S. Environmental Protection Agency (EPA) designated Cleco Corp.'s coal-fired Dolet Hills power plant in Mansfield out of compliance February 17 after determining that the plant emits too much sulfur dioxide. The utility must upgrade its facility in order to come into compliance with the EPA's standards.
   Source: http://www.bgdailynews.com/epa-cleco-coal-fired-power-plant-out-of-compliance/article_789b9d9d-2d14-5e8b-ac8b-44895a0d525f.html

2. *February 17, Santa Barbara Noozhawk* – (California) **Federal regulators determine external pipeline corrosion caused Refugio Oil Spill.** The Pipeline and Hazardous Materials Administration released a preliminary report February 17 which determined that external corrosion was the cause of the Refugio Oil Spill, a May 2015 incident where a ruptured Plains All American Pipeline leaked up to 142,800 gallons of crude oil onto the shoreline of southern Santa Barbara County and into the ocean. The agency ordered the company to shut down and purge the oil from two of its pipelines in the county due to concerns about corrosion.
   Source:
   http://www.noozhawk.com/article/phmsa_refugio_oil_spill_investigation_external_corrosion

3. *February 16, Northwest Indiana Post-Tribune* – (Indiana) **Security breach reported by Kankakee Valley REMC.** Indiana-based Kankakee Valley REMC announced February 16 that a foreign Internet Protocol (IP) address had accessed a storage device on the utility's network containing the personal information of 17,700 members. The utility immediately removed the accessed pathway and is uncertain if any information was copied or taken from the system.
   Source: http://www.chicagotribune.com/suburbs/post-tribune/news/ct-ptb-remc-computer-breach-st-0217-20160216-story.html

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

4. *February 18, Associated Press* – (International) **Toyota recalls 2.9M SUVs over seat belts.** Toyota Motor Corporation issued a recall February 18 for more than 1.1 million sports utility vehicles including its model years 2005 – 2014 RAV4 Sport Utility Vehicles (SUVs) and its model years 2012 – 2014 RAV4 electric vehicles sold in the U.S. due to potentially faulty seat belts in second-row window seats which could sever and/or fail to restrain passengers after coming into contact with a metal seat cushion

frame during a severe frontal crash. The recall affects an additional 1.8 million vehicles worldwide.
Source: http://www.usatoday.com/story/money/cars/2016/02/18/toyota-recalls-29m-suvs-over-seat-belts/80544376/

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *February 18, Portland Oregonian* – (National) **40,500 Oregonians hit by $25 million tax fraud scheme, feds say.** The U.S. Attorney's Office in Oregon announced February 17 that six individuals faces Federal charges for their roles in a $25 million tax-fraud scheme in which the men based on the East Coast stole the names, addresses, and Social Security numbers of over 250,000 people, 83,000 of which were stolen from Oregon-based CICS Employment Services database, and netted $4.7 million in profits. The group used the information to obtain electronic filing information from the Internal Revenue Service (IRS), filed fraudulent tax returns, and deposited the money using prepaid debit cards.
Source: http://www.oregonlive.com/pacific-northwest-news/index.ssf/2016/02/40500_oregonians_hit_by_25_mil.html

6. *February 17, U.S. Securities and Exchange Commission* – (California) **SEC charges biopesticide company and former executive with accounting fraud.** The U.S. Securities and Exchange Commission announced February 17 that Marrone Bio Innovations agreed to pay a $1.75 million penalty to settle charges that the Davis, California-based company and a former chief operating officer (COO) inflated financial results to meet its first year projections by concealing sales concessions from financial personnel and independent auditors and causing the company to improperly recognize revenue on sales at its business.
Source: https://www.sec.gov/news/pressrelease/2016-32.html

Transportation Systems Sector

7. *February 18, WDAF 4 Kansas City* – (Missouri) **WB I-70 re-opens after accident involving two tractor-trailers near Odessa.** Westbound lanes of Interstate 70 near Odessa were closed for 3 hours February 18 following an accident involving 2 semi-trucks.
Source: http://fox4kc.com/2016/02/18/wb-i-70-at-odessa-closed-due-to-accident-involving-two-tractor-trailers/

8. *February 18, Orlando Sentinel* – (Florida) **FHP: Woman killed in four-vehicle crash on I-4.** A fatal 4-vehicle crash that left one person dead and two others injured shut down all westbound lanes of Interstate 4 in Osceola County for several hours February 17 while crews worked to clear the wreckage.
Source: http://www.orlandosentinel.com/news/breaking-news/os-woman-dead-i4-

crash-world-drive-20160217-story.html

9. *February 17, WOAI 4 San Antonio* – (Texas) **WB loop 1604 reopened after 18-wheeler fire forces closure.** All lanes of Loop 1604 in San Antonio were reopened 10 hours after a semi-truck caught fire and prompted the closure of the highway February 17 while crews worked to clear the wreckage.
Source: http://news4sanantonio.com/news/local/traffic-alert-loop-1604-shut-down-near-blanco-road

10. *February 17, Associated Press* – (Massachusetts) **12-foot metal panel falls of Boston train, hits 3rd rail.** The State Street station on Massachusetts Bay Transportation Authority's (MBTA) Orange Line was evacuated along with two trains February 16 after a metal panel struck the electrified third rail filling the station with smoke and causing the two trains to become disabled after running over the panel. MBTA officials ordered inspections of all 120 Orange Line trains and found no major issues.
Source: http://www.fairfieldcitizenonline.com/news/us/article/Officials-MBTA-trains-evacuated-due-to-smoke-6835877.php

11. *February 17, Associated Press* – (Colorado) **Rock slide will keep Colorado highway mostly shut for weeks.** Colorado Department of Transportation officials announced February 17 that Interstate 70 from Glenwood Springs in the west to Gypsum in the east will be closed for several weeks while crews continue to remove loose rocks from the roadway following a February 15 rock slide that forced the interstate's closure.
Source: http://www.foxnews.com/us/2016/02/17/rock-slide-will-keep-colorado-highway-mostly-shut-for-weeks.html

For another story, see item **2**

Food and Agriculture Sector

12. *February 17, WCBS 2 New York City; Associated Press* – (Connecticut) **More than 200 pigs killed in devastating fire at Connecticut farm.** A February 16 fire at Maple Hill Farm in Cornwall, Connecticut, left more than 200 pigs dead and destroyed the barn after hanging lights reportedly ignited dry timbers and hay bales in a second-floor loft.
Source: http://newyork.cbslocal.com/2016/02/17/pigs-killed-maple-hill-farm-fire/

13. *February 17, U.S. Food and Drug Administration* – (National) **Lipari Foods issues voluntary recall of various retail and food service raw pistachio products due to potential Salmonella risk.** Lipari Foods, LLC issued a voluntary recall February 16 for several raw pistachio products sold in 21 variations after testing by its supplier International Foodsource, LLC, revealed the presence of Salmonella in raw pistachios products, which may pose potential contamination to items packaged from the affected lot. The products were distributed to food service and retail stores in 14 States.
Source: http://www.fda.gov/Safety/Recalls/ucm486489.htm

For another story, see item **6**

Water and Wastewater Systems Sector

14. *February 17, Baltimore Brew* – (Maryland) **Sewage overflow on Falls Road stopped, DPW says.** The Baltimore City Department of Public Works urged the public to avoid contact with urban streams due to possible pollution after an estimated 17,700 gallons of wastewater flowed into the Jones Falls from an overflowing sewer main. Crews removed trash and rags that had clogged the line.
Source: https://www.baltimorebrew.com/2016/02/17/sewage-overflow-on-falls-road-stopped-dpw-says/

15. *February 17, Greensboro News & Record* – (North Carolina) **More than 18,000 gallons of sewage spills into Eden's waters.** Excessive rain and melted snow caused 2 sewer overflows in Eden, North Carolina, February 16 allowing 10,300 gallons of untreated sewage to spill into Covenant Branch and approximately 7,800 gallons of untreated sewage to spill into Dry Creek.
Source: http://www.greensboro.com/news/local_news/more-than-gallons-of-sewage-spills-into-eden-s-waters/article_bf7eeaf3-240c-5ff6-b5d2-6fb296a156b6.html

Healthcare and Public Health Sector

16. *February 17, SC Magazine* – (California) **Magnolia Health Corporation suffers breach after falling for spoofed CEO email.** California-based Magnolia Health Corporation (MHC) notified employees from its five facilities after an unknown individual used the email address of MHC's CEO to request an Excel spreadsheet containing the personal information, including Social Security numbers, of employees. The health-care provider discovered the breach February 10 and notified employees February 12.
Source: http://www.scmagazine.com/magnolia-health-corporation-suffers-breach-after-falling-for-spoofed-ceo-email/article/475410/

17. *February 17, U.S. Department of Justice* – (National) **Fifty-one hospitals pay United States more than $23 million to resolve False Claims Act allegations related to implantation of cardiac devices.** The U.S. Department of Justice announced February 17 that it reached settlements with 51 hospitals in 15 States totaling more than $23 million for violations of the False Claims Act regarding the improper embedding of implantable cardioverter defibrillator (ICD) devices during periods prohibited by a National Coverage Determination (NCD) from 2003 to 2010. Officials determined that the hospitals did not abide by the predetermined waiting period provided by the NCD prior to the implantation of the devices.
Source: http://www.justice.gov/opa/pr/fifty-one-hospitals-pay-united-states-more-23-million-resolve-false-claims-act-allegations

18. *February 17, NBC News* – (Massachusetts; Florida) **Suspected hacker arrested after rescue at sea during Disney cruise.** A suspected hacker was arrested by the FBI in Miami February 17 and charged for allegedly assisting in an April 2014 computer attack on Boston Children's Hospital that took down the hospital's network and Web

site for several days, causing $300,000 in damage. Boston Children's Hospital released a statement acknowledging the attack and thanking the FBI for apprehending the hacker.
Source: http://www.nbcnews.com/news/us-news/suspected-hacker-arrested-after-rescue-sea-during-disney-cruise-n520131

19. *February 17, Los Angeles Times* – (California) **Hollywood hospital pays $17,000 in bitcoins to hackers who took control of computers.** Officials with Hollywood Presbyterian Medical Center in California announced February 17 that the hospital paid a $17,000 ransom in bitcoins February 15 to a hacker who used malware February 5 to infect and lock down the hospital's computer systems by encrypting files and demanding a ransom to obtain the decryption key. Hospital officials stated that all computer systems were restored and asserted that patient care and hospital records were never compromised.
Source: http://www.latimes.com/local/lanow/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Government Facilities Sector

See item **5**

Emergency Services Sector

Nothing to report

Information Technology Sector

20. *February 17, SecurityWeek* – (International) **Flaw allowed attackers to bypass FireEye detection engine.** FireEye released patches fixing an evasion technique vulnerability in its Virtual Execution Engine (VXE), Network Security (NX), Email Security (EX), File Content Security (FX), and Malware Analysis (AX) products after researchers from Blue Frost Security discovered that attackers could bypass the company's detection engine and temporarily whitelist malware by copying the system engine's binary into a virtual machine with the name "malware.exe" and rename the file to its original filename, which would avoid detection due to the lack of sanitization within the original filename. Once the file is labeled as non-malicious, its MD5 hash is added to a list of binaries that attackers can later use to attack the system with an arbitrary file name.
Source: http://www.securityweek.com/flaw-allowed-attackers-bypass-fireeye-detection-engine

21. *February 17, Softpedia* – (International) **26,000 WordPress sites leveraged in layer 7 DDoS attack.** A security researcher from Sucuri released instructions on how to prevent a new Layer 7 distributed denial-of-service (DDoS) attack on 26,000 WordPress Web sites that previously allowed attackers to abuse the WordPress WML-RPC service to throttle pingback requests to the victim's Web site while sending the pingback requests via Hypertext Transfer Protocol (HTTP), which forced the central

processing unit (CPU) to go into overdrive as it handled multiple encrypted connections.
Source: http://news.softpedia.com/news/26-000-wordpress-sites-leveraged-in-layer-7-ddos-attack-500552.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

Communications Sector

Nothing to report

Commercial Facilities Sector

22. *February 18, KFOR 4 Oklahoma City* – (Oklahoma) **Fire officials announce what caused large fire that consumed condo in N.W. Oklahoma City.** The Nantucket Condominiums and an adjacent building in Oklahoma City sustained extensive damage February 17 after a contractor conducting hot work on the exterior of the building accidentally sparked the blaze. All residents were safely evacuated and one firefighter sustained minor injuries.
Source: http://kfor.com/2016/02/18/fire-officials-announce-what-caused-large-fire-that-consumed-condo-in-n-w-oklahoma-city/

23. *February 17, KXAS 5 Fort Worth* – (Texas) **3-alarm fire leaves Dallas church in ruins.** Dallas Fire-Rescue officials reported February 17 that the Iglesia de Cristo Camino de Santidad was considered a total loss after a 3-alarm fire burned down the building. About 75 firefighters contained the fire and no injuries were reported.
Source: http://www.nbcdfw.com/news/local/2-Alarm-Fire-Engulfs-Church-369091891.html

24. *February 17, WRIC 8 Petersburg* – (Virginia) **Boiler room destroyed in fire at historic retreat center in Blackstone.** Officials believe boilers may have caused a February 17 fire at the Virginia United Methodist Assembly in Blackstone that heavily damaged the building and prompted five different fire departments to extinguish the blaze. An investigation remains ongoing to determine the exact cause of the blaze.
Source: http://wric.com/2016/02/17/boiler-room-destroyed-in-fire-at-historic-retreat-center-in-blackstone/

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.