Daily Open Source Infrastructure Report
03 March 2016

Top Stories

- The U.S. Department of Justice announced that the former chief executive officer (CEO) of Chesapeake Energy Corp was charged March 1 with conspiring to rig bids to buy oil and natural gas leases in Oklahoma from 2007 to 2012. – *Reuters* (See item **1**)

- Five New York residents were arrested in Rhode Island February 27 and March 1 after authorities found a total of 309 stolen credit cards and gift cards in the suspects' vehicles during traffic stops. – *WJAR 10 Providence* (See item **6**)

- Crews worked to contain an ethanol leak from a tanker that derailed on a Norfolk Southern line in the town of Ripley, New York, March 1. – *Associated Press* (See item **7**)

- Federal authorities announced March 1 that Qualcomm Incorporated agreed to pay $7.5 million to settle charges after officials found that the company provided full-time employment, paid internships, and kickbacks to Chinese government officials and their relatives in order to obtain business at government-owned telecom companies in China. – *U.S. Securities and Exchange Commission* (See item **20**)

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. *March 2, Reuters* – (Oklahoma) **Former Chesapeake CEO charged with bid-rigging of land leases.** The U.S. Department of Justice announced that the former chief executive officer (CEO) of Chesapeake Energy Corp was charged March 1 with conspiring to rig bids to buy oil and natural gas leases in Oklahoma by allegedly setting up a conspiracy involving two energy companies that agreed not to bid against each other in purchasing oil and natural gas leases in northwest Oklahoma from 2007 to 2012.
Source: http://www.reuters.com/article/us-usa-crime-mcclendon-idUSKCN0W35Y7

2. *March 2, Associated Press* – (North Dakota) **Underground tank leaks 10,000 gallons of gas into soil.** The North Dakota Department of Health announced March 1 that 10,000 gallons of premium gasoline leaked from an underground storage tank at a Bakken Oil Patch gas station along U.S. Highway 85 after gasoline was put into a Patriot Fuels LLC tank February 25. Officials are monitoring the site and requested that the company investigate the extent of the leak.
Source: http://www.wday.com/news/3960232-underground-tank-leaks-10000-gallons-gas-soil

3. *March 2, KING 5 Seattle; Associated Press* – (Washington) **Storm pounds western Washington, thousands without power.** Utility crews worked March 2 to restore power to 15,000 customers in western Washington who remained without service following severe storms March 1 which knocked out power to 75,000 customers due to thunderstorms and strong winds.
Source: http://www.king5.com/story/news/local/2016/03/01/strong-winds-topple-trees-knock-out-power/81176392/

For another story, see item **7**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

4. *March 1, Nuclear Street* – (Ohio) **NRC investigates two hiccups at Perry NPP.** The U.S. Nuclear Regulatory Commission reported February 29 that it began conducting a special investigation at the FirstEnergy Nuclear Operating Company-managed Perry Nuclear Power Plant in Ohio after two separate incidences in February caused a manual shut down of the reactor due to an increase in temperature in the suppression pool, and caused a temporary loss of power to certain plant cooling equipment.
Source: http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2016/03/01/nrc-investigates-two-hiccups-at-perry-npp-030102

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

5. *March 1, U.S. Attorney's Office, Eastern District of New York* – (International) **Chief executive officer of international metallurgical company arrested for exporting aerospace-grade metals to Iran.** New York officials reported that the chief executive officer (CEO) of Global Metallurgy LLC was arrested and charged March 1 for allegedly exporting a cobalt-nickel metallic powder used in aerospace, missile production, and nuclear applications, from the U.S. to Iran through an intermediary in Turkey on two occasions without the requisite approval from the U.S. Department of the Treasury's Office of Foreign Assets Control. Authorities reported that the CEO attempted to conceal the true destination of the goods from the U.S. supplier.
Source: https://www.justice.gov/usao-edny/pr/chief-executive-officer-international-metallurgical-company-arrested-exporting

Financial Services Sector

6. *March 1, WJAR 10 Providence* – (Rhode Island; Virginia) **Police seize at least 250 stolen credit cards in West Greenwich, Cranston.** Five New York residents were arrested in Rhode Island February 27 and March 1 after authorities found a total of 309 stolen credit cards and gift cards in the suspects' vehicles during traffic stops. Three of the culprits used the stolen credit cards to purchase $19,000 worth of merchandise in Virginia and the remaining two suspects used the stolen credit cards to purchase additional gift cards at local Stop & Shop Supermarkets.
Source: http://turnto10.com/news/local/police-seize-at-least-250-stolen-credit-cards-in-west-greenwich-cranston

Transportation Systems Sector

7. *March 2, Associated Press* – (New York) **Train derails in Ripley, NY; homes evacuated due to ethanol tanker leak.** Crews worked to contain an ethanol leak from a tanker that was part of 16 cars on a freight train that derailed on a Norfolk Southern line in the town of Ripley, New York, March 1. Officials stated that 25 to 30 people were evacuated as a precaution while cleanup work continued.
Source: http://www.syracuse.com/state/index.ssf/2016/03/train_derails_in_ripley_ny_crews_working_to_contain_ethanol_tanker_leak.html

8. *March 1, WXII 12 Winston-Salem* – (North Carolina) **Crash, spill close Interstate 77 north in Surry County.** Northbound lanes of Interstate 77 in Surry County were closed for several hours March 1 following an accident involving a semi-truck and a spill of an unknown substance.
Source: http://www.wxii12.com/news/Crash-spill-close-Interstate-77-north-in-Surry-County/38281886

Food and Agriculture Sector

Nothing to report

Water and Wastewater Systems Sector

9. *March 2, Wilmington Star-News* – (North Carolina) **Boil water advisory for northeast Brunswick.** Brunswick County Public Utilities issued a boil water advisory March 2 for Northwest, Sandy Creek, Leland, Navassa, and Belville following a water main break at the Bell Swamp Water Tank in Winnabow.
Source: http://www.starnewsonline.com/article/20160302/NEWS/160309951

10. *March 1, Gwinnett Daily Post* – (Georgia) **Debris blockage causes sewage spill near Chattahoochee tributary.** The Gwinnett County Department of Water Resources announced that debris in the sewer system caused approximately 6,681 gallons of sewage to spill from a manhole into a tributary of the Chattahoochee River in the Buford area February 29. Officials posted signs alerting residents and spread lime in an effort to reduce the effect of the spill.
Source: http://www.gwinnettdailypost.com/local/cities/buford/debris-blockage-causes-sewage-spill-near-chattahoochee-tributary/article_ce043be5-172b-51dc-9c6c-4efea03e41ef.html

Healthcare and Public Health Sector

11. *March 1, NJ.com* – (New Jersey) **Lead in Morristown hospital's tap water may have been there since January.** Atlantic Health System officials reported March 1 that patients, employees, and guests at Morristown Medical Center in New Jersey who ingested tap water at the hospital between January 22 – February 25 may have been exposed to lead following testing that found lead levels which exceeded mandated standards. The hospital is using bottled water for drinking and food preparation until further notice while authorities investigate the source of contamination.
Source: http://www.nj.com/morris/index.ssf/2016/03/lead_found_in_water_at_morristown_hospital_may_hav.html

Government Facilities Sector

12. *March 2, WTOP 103.5 FM Washington, D.C.* – (Virginia; Maryland; Washington, D.C.) **Thousands in area without power; Va. school closed.** William Ramsay Elementary School in Alexandria was closed March 2 due to a power outage that knocked out service to more than 3,400 customers in Maryland, Washington, D.C., and Virginia.
Source: http://wtop.com/local/2016/03/thousands-area-without-power-va-school-closed/

13. *March 1, San Francisco Chronicle* – (California) **Saratoga college gets 'all clear'**

after bomb-threat scare. Authorities spent nearly 5 hours investigating a bomb threat at West Valley College in Saratoga before issuing an all clear after school officials evacuated the campus and cancelled classes March 1.
Source: http://www.sfgate.com/crime/article/Credible-bomb-threat-prompts-evacuation-of-6863535.php

Emergency Services Sector

14. *March 2, WAPT 16 Jackson* – (Mississippi) **Accused killer takes guard hostage, escapes from Warren County Jail.** Authorities are searching for an inmate who escaped from the Warren County Jail in Vicksburg March 2 after he reportedly used a homemade shank and took a jailer hostage before exiting the jail.
Source: http://www.wapt.com/news/central-mississippi/accused-killer-takes-guard-hostage-escapes-from-warren-county-jail/38296208

Information Technology Sector

15. *March 2, Agence France-Presse* – (International) **NSA chief worries about cyber attack on US infrastructure.** The U.S. National Security Agency chief warned March 1 that attackers may try to execute a cyberattack against U.S. infrastructure similar to a 2015 Ukrainian incident in which a computer virus caused the networks of several regional electricity companies to go offline, and caused power grid failures throughout the country. Officials reported that partnerships between the public and private sectors were key to preventing such attacks.
Source: http://www.securityweek.com/nsa-chief-worries-about-cyber-attack-us-infrastructure

16. *March 1, SecurityWeek* – (International) **Kaspersky launches Targeted Attack protection platform.** Kaspersky Lab released its new solution, Kaspersky Anti Targeted Attack Platform which can help companies reduce the risk of advanced threats and targeted attacks, detect security breaches and attempts to penetrate entities' networks, and help organizations take immediate mitigation actions. The platform also helps predict where new targeted attacks will occur via an Advanced Sandbox, which provides an isolated environment for analysis of suspicious objects, as well as via a Targeted Attack Analyzer, which leverages data processing and machine learning technology to assess events and combine feedback from various analysis engines.
Source: http://www.securityweek.com/kaspersky-launches-targeted-attack-protection-platform

17. *March 1, SecurityWeek* – (International) **Microsoft unveils Advanced Threat Protection service.** Microsoft released its new service titled, Windows Defender Advanced Threat Protection which is designed to help organizations detect, investigate, and respond to advanced attacks on organizations' networks and will bring a post-breach layer of protection to the Windows 10 security platform by using Windows behavior sensors, cloud-based security analytics, and threat intelligence.
Source: http://www.securityweek.com/microsoft-unveils-advanced-threat-protection-service

18. *March 1, SecurityWeek* – (International) **Google's DLP for Gmail adds optical character recognition.** Google Inc., reported it will be releasing a new set of features for its Data Loss Prevention (DLP) for Gmail which will help administrators set DLP policies to analyze common image types and extract text for policy evaluation, in addition to improving attachment scanning, setting new predefined content detectors, and increasing control over content detection thresholds through new features such as Optical character recognition (OCR).
Source: http://www.securityweek.com/googles-dlp-gmail-adds-optical-character-recognition

19. *March 1, Help Net Security* – (International) **BluVector 2.0: Machine-learning malware detection.** Acuity Solutions reported it will be releasing its BluVector version 2.0, a malware detection solution, which will help companies identify threats, find previously unclassified and undetected attacks, and help security analysts understand how their organizations are being targeted within milliseconds. The threat detection appliance analyzes files from the Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP) protocols using BluVector's machine-learning classification engine and extracts features from each file to determine if the file is malicious based on the device's knowledge of benign and malicious files.
Source: https://www.helpnetsecurity.com/2016/03/01/bluvector-2-0-machine-learning-malware-detection/

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

20. *March 1, U.S. Securities and Exchange Commission* – (International) **SEC: Qualcomm hired relatives of Chinese officials to obtain business.** The U.S. Securities and Exchange Commission announced March 1 that Qualcomm Incorporated agreed to pay $7.5 million to settle charges that it violated the Foreign Corrupt Practices Act (FCPA) after the company provided full-time employment and paid internships to relatives of Chinese government officials in order to obtain business at government-owned telecom companies in China. Qualcomm Inc., also provided the officials with gifts, travel, and entertainment and misrepresented the bribes as legitimate business expenses in its records.
Source: https://www.sec.gov/news/pressrelease/2016-36.html

Commercial Facilities Sector

21. *March 2, WCVB 5 Boston* – (Massachusetts) **2 killed, 7 injured when SUV crashes**

into Sweet Tomatoes in Newton. Sweet Tomatoes Pizza in Newton, Massachusetts, sustained heavy damage March 1 after a vehicle crashed into the restaurant, killing two people and injuring seven others. The crash remains under investigation.
Source: http://www.wcvb.com/news/car-crashes-into-newton-restaurant/38284180

22. *March 1, WGRZ 2 Buffalo* – (New York) **3 arrests made in connection to overnight church fire.** Buffalo Police officials reported March 1 that three people were arrested and charged for arson, trespassing, and criminal mischief after the trio allegedly set fire in the rectory to the former Sacred Heart Church on the city's East Side, causing about $100,000 in damages. No injuries were reported and the incident was contained.
Source: http://www.wgrz.com/news/local/east-side/3-arrests-made-in-connection-to-overnight-church-fire/62385909

For another story, see item **6**

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 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.