Daily Open Source Infrastructure Report
02 November 2016

Top Stories

- Six individuals were charged October 31 for their roles in a more than $100 million money laundering scheme that operated in the U.S. and Mexico from approximately June 2011 – May 2016. – *U.S. Attorney's Office, Southern District of New York* (See item **9**)
- City leaders in Sacramento, California, announced October 29 that the Sacramento River Water Treatment Plant is running at full capacity following a 3-year, $165 million rehabilitation project. – *KCRA 3 Sacramento* (See item **14**)
- Google disclosed a Microsoft Windows zero-day local privilege escalation vulnerability in the Windows kernel that could allow attackers to escape the sandbox, and warned that the flaw is being exploited in the wild. – *Help Net Security* (See item **17**)
- Over 1,500 Ford Motor Company employees were evacuated and sent home from the Ford World Headquarters in Dearborn, Michigan, October 31 after a fire at an electrical substation in the building's basement that prompted officials to shut off power to the building. – *CNBC* (See item **20**)

Fast Jump Menu

Energy Sector

1. *November 1, Reuters* – (Alabama) **Colonial says main gasoline line could open by Saturday.** Colonial Pipeline Company reported November 1 that its main gasoline line may reopen as early as November 5 after an explosion and fire killed one worker and injured five others in Shelby County, Alabama, when a work crew hit Line 1 with a track hoe. The shutdown will restrict gasoline supplies to millions in the southeastern portion of the U.S.
   Source: http://www.reuters.com/article/us-pipeline-blast-alabama-idUSKBN12V2FC

2. *October 31, WHDH 7 Boston* – (Massachusetts) **Streets closed, buildings evacuated after Boston gas leak.** Crews worked October 31 to cap a gas leak near Government City Hall Plaza in Boston after contractors hit a 6-inch gas line, prompting officials to shut down surrounding roads and evacuate nearby businesses for several hours.
   Source: http://whdh.com/news/police-responding-to-report-of-gas-leak-in-boston/

3. *October 31, U.S. Environmental Protection Agency* – (Alaska) **EPA settles with Shoreside Petroleum for violating Federal clean air rules at fuel terminals in Seward and Cordova, Alaska.** The U.S. Environmental Protection Agency (EPA) reached October 31 an $89,000 settlement with Shoreside Petroleum, Inc. to resolve alleged violations of Clean Air Act rules at its fuel terminals in Seward and Cordova, Alaska, including the failure to install vapor capture and control systems on the Seward loading rack and on storage tanks at both terminals, and failure to limit gas loading to vapor-tight tank trucks, among other violations, that the company self-disclosed to the EPA in November 2014. To resolve the violations, the company spent approximately $402,000 to install and test pollution controls.
   Source: https://www.epa.gov/newsreleases/epa-settles-shoreside-petroleum-violating-federal-clean-air-rules-fuel-terminals-seward

For another story, see item 7

Chemical Industry Sector

4. *October 31, U.S. Environmental Protection Agency* – (International) **Chemical importer in Saddle Brook, New Jersey settles chemical reporting case with EPA.** The U.S. Environmental Protection Agency (EPA) announced October 31 that it reached a $143,300 settlement with Mitsuya Boeki USA, Inc. to resolve alleged violations of Federal rules requiring producers and importers to provide the EPA with information on the production and use of large amounts of chemicals after an EPA inspection of the company's Saddle Brook, New jersey facility revealed that the business failed to report its importation of 7 chemicals subject to the reporting rule. As part of the settlement, the company filed a revised report and will institute management practices to guarantee compliance with all future provisions of Federal toxics laws and regulations.
   Source: https://www.epa.gov/newsreleases/chemical-importer-saddle-brook-new-jersey-settles-chemical-reporting-case-epa

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

5. *October 31, U.S. Department of Labor* – (Ohio) **Ohio trailer lining manufacturer faces nearly $215K in fines after OSHA finds company disabled safety devices, exposed workers to hazards.** The Occupational Safety and Health Administration cited Ridge Corporation with 1 willful, 2 repeated, 6 serious, and 1 other-than-serious citation October 26 after a 2015 investigation at the Pataskala, Ohio facility revealed that the company failed to install machine guards on multiple pieces of equipment, remove defective forklifts from service, and cover exposed electrical connections, among other violations. Proposed penalties total $214,857.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=33372

6. *October 31, U.S. Department of Labor* – (Texas) **OSHA investigation of two serious employee injuries finds global filtration manufacturer failed to protect workers from safety and health hazards.** The Occupational Safety and Health Administration cited PECOFacet with 21 serious violations October 31 after an investigation into 2 employee injuries at the company's Mineral Wells, Texas plant in April and May 2016 revealed that the company allowed equipment to operate without safety latches, permitted the use of non-compliant crane equipment, and failed to address electrical hazards, among other violations. Proposed penalties total $224,477.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=33366

Defense Industrial Base Sector

See item **6**

Financial Services Sector

7. *October 31, U.S. Securities and Exchange Commission* – (Minnesota; North Dakota) **Company co-founder charged in manipulation scheme.** The U.S. Securities and Exchange Commission charged October 31 the co-founder of Minnesota-based Dakota Plains Holdings Inc. for orchestrating a scheme where he and co-conspirators allegedly siphoned $32 million from the company by concealing his control of the company, manipulating the company's stock prices, and issuing millions of shares to himself, family, and friends. Dakota Plains' co-founder agreed to pay almost $8 million to resolve allegations that he acquired illicit payments and evaded public disclosure requirements by disseminating his company's stock holdings across 10 accounts in various names to hide his ownership of over 20 percent of the firm's shares and his accumulation of millions of dollars in bonus payments.

Source: https://www.sec.gov/news/pressrelease/2016-231.html

8. *October 31, U.S. Securities and Exchange Commission* – (California) **Audit partner charged in failed audits of venture capital fund.** The U.S. Securities and Exchange Commission announced October 31 proceedings against a PricewaterhouseCoopers LLP audit partner after the partner allegedly failed to scrutinize millions of dollars taken from Burrill Life Sciences Capital Fund III, LP during independent audits, failed to establish whether the fund's adviser had appropriate authorization and reasoning for taking the money, and neglected to confirm that the transactions were accurately disclosed in the fund's financial statements. The money taken from the venture capital fund was allegedly used by the owner and principal of the investment adviser to cover personal and business expenses.
Source: https://www.sec.gov/news/pressrelease/2016-230.html

9. *October 31, U.S. Attorney's Office, Southern District of New York* – (International) **Manhattan U.S. Attorney announces charges against six individuals for their role in international money laundering scheme involving over $100 million.** Six individuals were charged October 31 for their roles in a more than $100 million money laundering scheme where the group allegedly caused front companies in Mexico to export outdated cell phones to other shell companies in the U.S., and created export documents that falsely inflated the value of the exported phones in order to deceitfully obtain value added tax (VAT) refunds from the Mexican government from about June 2011 – May 2016. The charges allege that each mobile phone transfer was accompanied by a transfer of funds to and from accounts in the names of the relevant front companies owned and controlled by the group in order to make the cell phone sales appear legitimate.
Source: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-six-individuals-their-role

Transportation Systems Sector

10. *November 1, WWJ 62 Detroit* – (Michigan) **Driver thrown from vehicle, killed in overnight crash on I-96.** Eastbound Interstate 96 at Livernois Avenue in Detroit was closed for several hours November 1 following a rollover crash involving three vehicles. One person was killed and the cause of the crash remains under investigation.
Source: http://detroit.cbslocal.com/2016/11/01/driver-thrown-from-vehicle-killed-in-overnight-crash-on-i-96/

11. *November 1, WJZ 13 Baltimore* – (Maryland) **6 dead, 10 hospitalized after MTA bus, school bus collide in SW Baltimore.** Six people were killed and 10 others were transported to area hospitals November 1 after a school bus crashed into another vehicle and a pillar before striking an oncoming Maryland Transit Administration bus on Frederick Avenue in southwest Baltimore. No students were on the school bus at the time of the crash and the incident remains under investigation.
Source: http://baltimore.cbslocal.com/2016/11/01/mta-bus-crashes-with-school-bus-in-southwest-baltimore/

12. *October 31, Fresno Bee* – (California) **Big boulders block El Portal Road to Yosemite National Park.** Highway 140 into Yosemite National Park in California was closed until further notice October 31 after several large boulders fell onto the highway. Crews were working to remove the rocks and officials were assessing the stability of the slope above the rock fall.
Source: http://www.fresnobee.com/news/local/article111717312.html

13. *October 31, WSAV 3 Savannah* – (Georgia) **More than 10 hour standoff comes to an end.** A portion of Highway 57 south of Ludowici, Georgia, was closed for more than 10 hours October 31 after authorities stopped a Long County robbery suspect who claimed to have explosives, prompting the response of bomb disposal teams. The incident remains under investigation.
Source: http://wsav.com/2016/10/31/10-hours-long-county-standoff-continues/

For another story, see item **6**

Food and Agriculture Sector

Nothing to report

Water and Wastewater Systems Sector

14. *October 30, KCRA 3 Sacramento* – (California) **Sacramento River Water Treatment Plant back at full capacity.** City leaders in Sacramento, California, announced October 29 that the Sacramento River Water Treatment Plant is running at full capacity following a 3-year, $165 million rehabilitation project that replaced the plant's old machinery, enabling it to treat up to 160 million gallons of water per day.
Source: http://www.kcra.com/article/sacramento-river-water-treatment-plant-back-at-full-capacity/8009480

For another story, see item **6**

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

15. *October 31, WTNH 8 New Haven* – (Connecticut) **Bomb threat forces early dismissal of Hamden High School.** Students at Hamden High School in Hamden, Connecticut, were evacuated and dismissed October 31 following a bomb threat. Authorities searched the school and the threat remains under investigation.
Source: http://wtnh.com/2016/10/31/hamden-high-school-dismissing-early-while-police-search-building/

16. *October 31, Anniston Star* – (Alabama) **Crews fighting wildfire in Talladega National Forest as drought continues.** Crews worked October 31 to contain the roughly 800-acre wildfire burning in the Talladega National Forest in Alabama. U.S.

Forest Service crews were working to set up a 1,000-acre perimeter to prevent the fire from spreading.
Source: http://www.annistonstar.com/news/local/crews-fighting-wildfire-in-talladega-national-forest-as-drought-continues/article_f57e931c-9fa9-11e6-85db-1bab91f6d1c6.html

For additional stories, see items **11** and **12**

Emergency Services Sector

Nothing to report

Information Technology Sector

17. *November 1, Help Net Security* – (International) **Google warns of actively exploited Windows zero-day.** Google disclosed a Microsoft Windows zero-day local privilege escalation vulnerability in the Windows kernel that could allow attackers to escape the sandbox. Google researchers warned that the flaw is being actively exploited in the wild.
Source: https://www.helpnetsecurity.com/2016/11/01/google-warns-actively-exploited-windows-zero-day/

18. *October 31, SecurityWeek* – (International) **Nymaim starts using PowerShell to download payload.** Verint security researchers discovered the Nymaim malware dropper received updates and is now delivered via spear-phishing emails carrying Macro-enabled Microsoft Word documents, uses PowerShell to download a first-stage payload, includes more effective obfuscation methods, and abuses MaxMind to avoid detection by security software. If the MaxMind query response includes a string of interest, such as the names of security vendors, the first stage Nymaim payload is not downloaded.
Source: http://www.securityweek.com/nymaim-starts-using-powershell-download-payload

19. *October 31, IDG News Service* – (International) **Joomla websites attacked en masse using recently patched exploits.** Sucuri security researchers discovered that malicious actors were exploiting two critical vulnerabilities patched in Joomla 3.6.4 to create accounts with elevated privileges on Websites built with the Joomla content management system, even in cases where registration is disabled. Sucuri researchers reported that nearly every Joomla Website on its network was impacted and between October 26 and October 28, there were roughly 28,000 attacks.
Source: http://www.computerworld.com/article/3136932/security/joomla-websites-attacked-en-masse-using-recently-patched-exploits.html#tk.rss_security

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

20. *October 31, CNBC* – (Michigan) **Fire at Ford World Headquarters forces evacuation.** Over 1,500 Ford Motor Company employees were evacuated and sent home from the Ford World Headquarters in Dearborn, Michigan, October 31 after a fire at an electrical substation in the building's basement that prompted officials to shut off power to the building. No injuries were reported and the cause of the fire remains under investigation.
Source: http://www.cnbc.com/2016/10/31/fire-at-ford-world-headquarters-forces-evacuation.html

For another story, see item 2

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