Daily Open Source Infrastructure Report
22 November 2016

Top Stories

- JPMorgan Chase & Co. agreed November 17 to pay a total of more than $264 million to resolve charges stemming from alleged violations of the Foreign Corrupt Practices Act. – *U.S. Securities and Exchange Commission* (See item **2**)
- Officials reported that more than 200,000 gallons of wastewater spilled into Rocky Creek in Tampa, Florida, November 18 after bypass piping failed during valve replacement work. – *Tampa Bay Times* (See item **13**)
- Michigan State University officials reported November 18 that an unauthorized party breached one of its servers November 13 and accessed a database containing 400,000 records containing the names, Social Security numbers, and birthdates of current and former students and employees. – *SecurityWeek; WSYM 47 Lansing* (See item **14**)
- More than 6,300 firefighters continued working November 20 to contain wildfires that have collectively burned more than 119,000 acres across 8 southeastern States. – *Knoxville News Sentinel* (See item **15**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

See item **12**

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

1. *November 18, Pocono Record* – (Pennsylvania) **Two charged with stealing credit card info in Monroe County.** Two men were charged November 17 for allegedly stealing credit card account information and transferring the information onto fraudulent credit cards after authorities discovered 78 suspected fake credit cards, a credit card embossing machine, and 2 card skimming devices, among other illicit items, at one of the co-conspirator's residence in Tobyhanna, Pennsylvania.
   Source: http://www.poconorecord.com/news/20161118/two-charged-with-stealing-credit-card-info-in-monroe-county

2. *November 17, U.S. Securities and Exchange Commission* – (International) **JPMorgan Chase paying $264 million to settle FCPA charges.** The U.S. Securities and Exchange Commission announced November 17 that JPMorgan Chase & Co. agreed to pay a total of more than $264 million to resolve charges stemming from alleged violations of the Foreign Corrupt Practices Act (FCPA) after the company reportedly won business from clients and corruptly influenced government officials in the Asia-Pacific region by providing their friends and family members with jobs and internships over the course of 7 years. According to the settlement, JPMorgan hired around 100 interns and full-time personnel at the request of foreign government officials, enabling the company to accumulate over $100 million in revenues from winning or retaining business.
   Source: https://www.sec.gov/news/pressrelease/2016-241.html

Transportation Systems Sector

3. *November 21, WNCN 17 Goldsboro* – (North Carolina) **Tractor-trailer carrying**

bananas flips over on I-85 in Hillsborough after driver falls asleep. A portion of Interstate 85 in Hillsborough, North Carolina, was closed for more than 5 hours November 21 after a semi-truck struck a guardrail and overturned when the driver fell asleep, causing debris and its load of bananas to spill across the roadway. No injuries were reported.
Source: http://wncn.com/2016/11/21/lanes-closed-in-section-of-i-85-after-truck-carrying-bananas-flips-in-hillsborough/

4. *November 21, Syracuse Post-Standard* – (National) **Snow, wind causes some delays, cancellations at Syracuse's Hancock airport.** A total of 9 flights arriving at or departing from the Syracuse Hancock International Airport in New York were canceled and 13 others were delayed November 21 following winter storms that moved through central New York and the northeast November 20.
Source: http://www.syracuse.com/news/index.ssf/2016/11/snow_wind_causes_some_delays_cancelations_at_syracuses_hancock_airport.html

5. *November 20, KFSN 30 Fresno* – (California) **Highway 99 partially closed in Fresno after fatal crash.** Two northbound lanes of Highway 99 in Fresno, California, were closed for more than 4 hours November 20 following a collision that killed at least 1 person. The crash remains under investigation.
Source: http://abc30.com/traffic/highway-99-partially-closed-in-fresno-after-fatal-crash/1617507/

6. *November 19, KMOV 4 St. Louis* – (Missouri) **Police: Suspect shot himself after crashing stolen vehicle, shutting down I-270.** Both directions of Interstate 270 in St. Louis were closed for several hours November 19 after a suspect driving a stolen vehicle crashed during a police pursuit and then shot himself. Two other passengers were taken into custody and the driver was transported to an area hospital.
Source: http://www.kmov.com/story/33750612/nb-i-270-reopens-following-police-chase-ending-in-crash-sb-lanes-closed

7. *November 19, Bemidji Pioneer* – (Minnesota) **Semi, SUV crash temporarily closes Highway 71.** A head-on collision involving a semi-truck and another vehicle forced the closure of U.S. Route 71 in Hubbard County, Minnesota, for several hours November 19.
Source: http://www.bemidjipioneer.com/news/4163168-updated-semi-suv-crash-temporarily-closes-highway-71

For additional stories, see items **20** and **25**

Food and Agriculture Sector

8. *November 19, U.S. Food and Drug Administration* – (International) **H-E-B issues precautionary baby food recall.** H-E-B Grocery Company, LP issued a precautionary recall November 18 for all of its H-E-B Baby Food 2-pack products sold in 4-ounce cups after the firm received a customer report stating that a small rubber piece was

found inside a single container of one variety of the product. H-E-B is investigating the incident and no illnesses or injuries have been reported.
Source: http://www.fda.gov/Safety/Recalls/ucm529966.htm

9. *November 19, U.S. Food and Drug Administration* – (International) **Sabra Dipping Company issues voluntary recall of certain hummus products because of possible health risks.** Sabra Dipping Co., LLC issued a voluntary recall November 19 for several variations of its hummus products after Listeria monocytogenes was found at the company's manufacturing facility. The products were distributed to retail establishments, including food service accounts and supermarkets, nationwide and in Canada.
Source: http://www.fda.gov/Safety/Recalls/ucm529967.htm

10. *November 19, U.S. Department of Agriculture* – (National) **Wayne Farms LLC. recalls ready-to-eat chicken breast products that may be undercooked.** Wayne Farms LLC issued a recall November 18 for roughly 4,059 pounds of its "Fully Cooked Grilled Chicken Breast Fillets" sold in 9-pound bulk cases and its "Fully Cooked Flame Grilled Chicken Breast Fillets" sold in 22.5-pound bulk cases due to undercooking after a routine records review by the firm revealed that a similar product appeared to be undercooked. There have been no confirmed reports of adverse health effects and the products were shipped to retail outlets in five States.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-110-2016-release

11. *November 18, Food Safety News; Inland Valley Daily Bulletin* – (National) **Dr. Bob's closes in wake of ice cream recalls for Listeria.** Dr. Bob's Handcrafted Ice Cream removed its Website November 17 and the firm's Pomona, California-based operation shut down in October after Federal inspectors discovered Listeria monocytogenes in the production facility and in finished products, prompting 4 of the company's corporate customers to issue secondary recalls of 5 brands of premium ice cream products that were shipped nationwide.
Source: http://www.foodsafetynews.com/2016/11/dr-bobs-closes-in-wake-of-ice-cream-recalls-for-listeria/#.WDL977IrKUk

Water and Wastewater Systems Sector

12. *November 21, WKTV 2 Utica* – (New York) **Hazmat crews return to Rome water treatment plant after second chlorine leak.** Rome, New York officials reported that a 30-pound chlorine leak inside the city's new water treatment plant November 19 and a subsequent leak November 21 sent 2 individuals to the hospital and prompted emergency and HAZMAT crews to respond from November 19 – November 21. Officials reported that no chlorine leaked into the water supply and the leaks were contained inside the building.
Source: http://www.wktv.com/news/hazmat_Rome_chlorine_leak.html

13. *November 19, Tampa Bay Times* – (Florida) **Hillsborough utilities: More than 200,000 gallons of wastewater discharged into Rock Creek.** Hillsborough County

Public Utilities officials reported that more than 200,000 gallons of wastewater spilled into Rocky Creek in Tampa, Florida, November 18 after bypass piping failed during valve replacement work. Officials advised people not to fish, wade, or swim in Rocky Creek or in the vicinity of where the creek flows into Tampa Bay.
Source: http://www.tampabay.com/news/publicsafety/hillsborough-utilities-more-than-200000-gallons-of-wastewater-discharged/2303468

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

14. *November 21, SecurityWeek; WSYM 47 Lansing* – (Michigan) **400,000 records exposed in Michigan State University breach.** Michigan State University (MSU) officials reported November 18 that an unauthorized party breached one of its servers November 13 and accessed a database containing 400,000 records containing names, Social Security numbers, and birthdates of current and former students and employees, among other personal information. The hackers reportedly attempted to extort the university after accessing the database, and officials believe only a few hundred records were actually stolen.
Source: http://www.securityweek.com/400000-records-exposed-michigan-state-university-breach

15. *November 20, Knoxville News Sentinel* – (National) **Forest fires burn 119,000 acres in 8 southeastern states.** More than 6,300 firefighters continued working November 20 to contain wildfires that have collectively burned more than 119,000 acres across 8 southeastern States.
Source: http://www.usatoday.com/story/news/nation-now/2016/11/20/forest-fires-burn-119000-acres-8-southeastern-states/94169774/

16. *November 19, Brockton Enterprise* – (Massachusetts) **Smoky fire causes $40G damage at Whitman-Hanson High.** A fire in a commercial dryer at Whitman-Hanson Regional High School in Hanson, Massachusetts, caused an estimated $40,000 in smoke and water damage November 19. Officials reported the fire started due to a lint buildup underneath the dryer.
Source: http://www.enterprisenews.com/news/20161119/smoky-fire-causes-40g-damage-at-whitman-hanson-high

17. *November 18, Boston Globe* – (Massachusetts) **Police say report of gunman at BU a hoax.** The Mugar Memorial Library and adjacent George Sherman Union at Boston University were evacuated for about 2 hours November 18 after a man called the university's police stating he was barricaded in the library with weapons and explosives and had shot someone. Authorities determined the call was a hoax after searching the facility.
Source: https://www.bostonglobe.com/metro/2016/11/18/authorities-investigate-potential-emergency-situation-building/R3QvWqhASCQuoPIoAhovQP/story.html

For another story, see item **20**

Emergency Services Sector

Nothing to report

Information Technology Sector

18. *November 21, Help Net Security* – (International) **Malware masquerading as an image spreads via Facebook.** A malware researcher discovered malware is spreading via Facebook in the form of Scalable Vector Graphics (SVG) image files that contain embedded content and are automatically sent from compromised user accounts in order to redirect users to a Website impersonating YouTube where a victim is required to install a specific codec extension before viewing the video, which gives the malware the capability to alter a user's data on the Websites they visit. The researcher reported the SVG file also contains the Nemucod downloader; however it has not been spotted downloading the Locky ransomware or other malware.
Source: https://www.helpnetsecurity.com/2016/11/21/malware-image-facebook/

19. *November 21, SecurityWeek* – (International) **Palo Alto Networks patches flaws found by Google researcher.** Palo Alto Networks, Inc. patched several vulnerabilities in its PAN-OS operating system after a Project Zero researcher found three security flaws affecting the products including an issue that could allow an attacker with network access to the Web management interface to execute arbitrary code or cause a denial-of-service (DoS) condition due to how the Web management server handles a buffer overflow. The patches also addressed two local privilege escalation bugs that could be exploited to obtain root permissions, an OpenSSH flaw, and a post-authentication flaw that could allow XPath manipulation.
Source: http://www.securityweek.com/palo-alto-networks-patches-flaws-found-google-researcher

20. *November 20, Softpedia* – (International) **Microsoft Xbox, PlayStation, other popular Twitter accounts hacked.** Twitter Counter confirmed its service experienced a security breach and several high-profile Twitter accounts, including those owned by Microsoft Xbox, the U.S. National Transportation Safety Board, and the Minnesota governor, among others were hacked to post links to services that increase a user's number of followers for other accounts. Twitter Counter stated an investigation into the breach is ongoing and the hackers can no longer post on another user's behalf.
Source: http://news.softpedia.com/news/microsoft-xbox-playstation-other-popular-twitter-accounts-hacked-510357.shtml

21. *November 18, SecurityWeek* – (International) **Over-the-air update mechanism exposes millions of Android devices.** Security researchers reported that over 2.8 million Android devices across 55 device models were vulnerable to Man-in-the-Middle (MitM) attacks and could allow a remote, unauthenticated attacker to replace server responses with their own and execute arbitrary commands as root on the device due to an insecure implementation of the over-the-air (OTA) update mechanism from

Ragentek Group, which failed to use an encrypted channel for transactions from the binary to third-party endpoint.
Source: http://www.securityweek.com/over-air-update-mechanism-exposes-millions-android-devices

22. *November 18, SecurityWeek* – (International) **Moxa, Vanderbilt surveillance products affected by serious flaws.** The Industrial Control Systems-Computer Emergency Readiness Team (ICS-CERT) released an advisory which reported that Moxa's SoftCMS central management software was plagued with three serious vulnerabilities after security researchers discovered a Structured Query Language (SQL) injection flaw that could be remotely exploited to access the software with administrator privileges, a double free condition that could lead to a denial-of-service (DoS) condition, and an improper input validation flaw that could lead to a crash of the application. ICS-CERT and Siemens also informed customers that several Siemens-brand Vanderbilt IP cameras were affected by a flaw that could allow an attacker with network access to obtain administrative privileges using maliciously crafted requests.
Source: http://www.securityweek.com/moxa-vanderbilt-surveillance-products-affected-serious-flaws

23. *November 17, Help Net Security* – (International) **Ransoc browser locker/ransomware blackmails victims.** Security researchers discovered the Ransoc ransomware is being distributed via malvertising to target and blackmail Microsoft Windows users who frequent adult Websites, and scans an infected device to collect information from the victim's Facebook, LinkedIn, and Skype accounts, as well as scans local media filenames for strings associated with files downloaded via torrents in order to uncover illegal or illicit content. The ransomware then displays a ransom note, or "penalty notice" tailored to the information it finds, threatening to expose a victim's illicit online activity to the user's social and professional network connections if the fine is not paid.
Source: https://www.helpnetsecurity.com/2016/11/17/ransoc-browser-lockerransomware-blackmails-victims/

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

24. *November 20, Time Warner Cable News* – (New York) **Multiple businesses suffer significant damage in plaza fire.** A 3-alarm fire damaged several businesses at the

Mount Hope Plaza in Rochester, New York, November 19. No injuries were reported and authorities believe the fire began at the Jing Li Chinese Restaurant, which sustained significant damage.
Source: http://www.twcnews.com/nys/rochester/news/2016/11/20/mount-hope-plaza-fire.html

25. *November 20, Orange County Register* – (California) **Fire in Anaheim destroys 7 tractor-trailers.** Authorities are investigating a 2-alarm fire at a tractor-trailer yard in Anaheim, California, November 19 that destroyed 7 semi-trucks, caused over $500,000 in damages, and forced the closure of nearby roads for several hours. No injuries were reported and the cause of the fire is under investigation.
Source: http://www.ocregister.com/articles/tractor-736056-fire-anaheim.html

26. *November 20, WJZ 13 Baltimore* – (Maryland) **Club house destroyed by fire at Willow Springs Golf Course.** The clubhouse at the Willow Springs Golf Course in Sykesville, Maryland, was considered a total loss after a November 20 fire. No injuries were reported.
Source: http://baltimore.cbslocal.com/2016/11/20/club-house-destroyed-by-fire-at-willow-springs-golf-course/

27. *November 19, KARE 11 Minneapolis* – (Minnesota) **Fire destroys Baxter auto parts store during snowstorm.** Dean's Auto Parts store in Baxter, Minnesota, was considered a total loss after a fire broke out November 18. No injuries were reported and the cause of the fire remains under investigation.
Source: http://www.kare11.com/news/local/fire-destroys-baxter-auto-parts-store-during-snowstorm/354113511

28. *November 18, WTAE 4 Pittsburgh* – (Pennsylvania) **18 apartments damaged in Middle Hill fire.** A 4-alarm apartment fire in the Middle Hill neighborhood of Pittsburgh displaced roughly 21 people and damaged 18 units November 18. No injuries were reported.
Source: http://www.wtae.com/article/middle-hill-row-houses-up-in-flames/8341643

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