Daily Open Source Infrastructure Report
05 August 2016

Top Stories

- A former teller at a TD Bank branch in Washington Township, New Jersey, pleaded guilty to Federal charges August 2 after she embezzled $608,000 from 8 bank customers between 2014 and 2015. – *Cherry Hill Courier-Post* (See item **3**)
- Maryland officials announced August 3 that a broken sewer line in Ellicott City is dumping nearly 5 million gallons of sewage per day into a Patapsco River tributary following flash floods that hit the city July 30. – *WUSA 9 Washington, D.C.* (See item **16**)
- Duke Energy officials reported August 3 that up to 50,000 gallons of storm water runoff spilled from their coal-fired power plant in Rutherford County, North Carolina, into the Broad River. – *Associated Press* (See item **17**)
- Banner Health notified approximately 3.7 million patients, health plan members, physicians, and health care providers August 3 of a potential data breach after hackers may have gained unauthorized access to patient, physician, and beneficiary data in its computer systems between June 23 and July 7. – *Reuters* (See item **18**)

Fast Jump Menu

Energy Sector

See item **17**

Chemical Industry Sector

See item **5**

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

Critical Manufacturing Sector

1. *August 3, U.S. Department of Labor* – (Ohio) **OSHA finds Ohio metal coating plant continues to expose workers to risk of injuries, illnesses from acid, chemical, machine hazards.** The Occupational Safety and Health Administration cited Moore Chrome Products Company, doing business as Moore Metal Finishing, with 1 willful, 5 repeated, and 4 serious violations July 29 after a February investigation at the Sylvania, Ohio facility revealed that the company failed to provide medical surveillance to employees exposed to hazardous chemicals, failed to follow respiratory protection standards, and failed to label acid tanks, among other violations. Proposed penalties total $115,000.
   Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=32949

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

2. *August 3, Softpedia* – (International) **Venmo fixes hole that allowed attackers to steal $2,999.99 per week using Siri.** Venmo patched an attack vector in its digital wallet service after a security researcher discovered attackers could exploit design flaws in Venmo and Apple's iPhone operating system (iOS) to approve roughly $3,000 a week in money requests if a malicious actor had physical access to a victim's iPhone by instructing Siri to send a message to a Venmo five-digit phone number on an iOS device that would handle the payment request instead of showing app notifications to the user. Venmo removed the Short Message Service (SMS) "reply-to-pay" functionality, as well as other smaller patches that made the service vulnerable to similar attacks.
   Source: http://news.softpedia.com/news/venmo-fixes-hole-that-allowed-attackers-to-steal-2-999-99-per-week-using-siri-506912.shtml

3. *August 2, Cherry Hill Courier-Post* – (New Jersey) **Washington Twp. TD Bank teller**

admits to $600K scam. A former teller at a TD Bank branch in Washington Township, New Jersey, pleaded guilty to Federal charges August 2 after she embezzled $608,000 from 8 bank customers between 2014 and 2015 by transferring money from dormant checking accounts into personal bank accounts or by obtaining cashier's checks issued in her name. Officials stated the former teller used the stolen funds for personal use.
Source: http://www.courierpostonline.com/story/news/2016/08/02/washington-twp-td-bank-teller-admits-600k-scam/87972636/

Transportation Systems Sector

4. *August 4, WQAD 8 Moline* – (Iowa) **Crash near Blue Grass closes southbound Highway 61 for several hours.** Southbound lanes of Highway 61 in Blue Grass, Iowa, were closed for approximately 5 hours August 4 while officials investigated the scene of a crash.
Source: http://wqad.com/2016/08/04/breaking-news-crash-closes-highway-61-south-near-blue-grass-ia/

5. *August 3, KOMO 4 Seattle/KIMA 29 Yakima*– (Washington) **Authorities identify man killed in fiery crash near Cle Elum Wednesday.** A stretch of Interstate 90 in Cle Elum, Washington, was closed for several hours August 3 after a semi-truck carrying 4 tanks of anhydrous ammonia overturned and was struck by another vehicle, causing one of the 1,000 gallon tanks to rupture and leak. Officials evacuated the Indian John rest area and nearby homes as a precaution.
Source: http://keprtv.com/news/local/i-90-closed-east-of-cle-elum-after-fiery-car-semi-crash-kills-1-08-03-2016

6. *August 3, WCSM 96.7 FM Celina*– (Ohio) **Greenville teenager killed in accident that closed US 127 on Tuesday.** Highway 127 in Greenville, Ohio, was closed for several hours August 2 while officials assessed the scene of a two-vehicle accident that left one person dead and sent four others to area hospitals.
Source: http://www.wcsmradio.com/index.php/news/19216/117/Greenville-teenager-killed-in-accident-that-closed-US-127-on-Tuesday

7. *August 3, Chillicothe Gazette* – (Ohio) **Semi crash reduces U.S. 23 to one lane for two hours.** Highway 23 in Chillicothe, Ohio, was reduced to one lane for 2 hours August 3 while crews worked to clean up an oil spill following a crash involving two semi-trucks that left one driver with minor injuries.
Source: http://www.chillicothegazette.com/story/news/local/2016/08/03/semi-crash-reduces-us-one-lane-two-hours/88041332/

8. *August 3, Massillon Independent* – (Ohio) **Rescue crews free driver trapped after two trucks collide on Route 30.** Eastbound lanes of Route 30 in Dalton, Ohio, were closed for about 3 hours August 3 while officials investigated a two-vehicle crash that sent both vehicles into a ditch and trapped one driver in his vehicle for about an hour.
Source: http://www.indeonline.com/news/20160803/rescue-crews-free-driver-trapped-after-two-trucks-collide-on-route-30

9. *August 3, WNDU 16 South Bend* – (Indiana) **Spilled paint closes the eastbound Indiana Toll Road for six hours.** Indiana Toll Road eastbound near Bristol, Indiana, was closed for about 6 hours August 3 while crews worked to clean up approximately 23,000 pounds of white latex paint that spilled on the roadway after a semi-truck carrying the paint left the roadway and overturned. The driver was sent to the hospital with injuries.
Source: http://www.wndu.com/content/news/BREAKING-East-bound-Toll-Road-near-Bristol-closed-due-to-semi-rollover-crash-paint-spill-389067811.html

10. *August 3, KSNV 3 Las Vegas* – (California) **One killed after semi crashes into parked truck on northbound I-15 south of Primm.** Interstate 15 in Halloran Spring, California, was closed in both directions for several hours August 3 following an accident involving two semi-trucks that left one person dead and sent three others to an area hospital. HAZMAT crews responded after authorities noticed a strong smell of chlorine.
Source: http://news3lv.com/news/local/one-person-killed-after-2-semis-crash-on-i-15-south-of-primm

11. *August 3, WITN 7 Washington* – (North Carolina) **Highway 24 re-opens in Duplin County after tanker crash.** Highway 24 in Duplin County, North Carolina, was closed for several hours August 3 after a tanker truck carrying 1,500 gallons of diesel and 500 gallons of gasoline overturned, causing the tank to separate from the tanker. The driver was transported to an area hospital with non-life-threatening injuries.
Source: http://www.witn.com/content/news/Highway-24-closed-in-Duplin-County-after-tanker-crash-389077462.html

12. *August 3, WXII 12 Winston-Salem* – (North Carolina) **Tractor-trailers involved in I-77 crash in Surry County.** Interstate 77 north was closed for more than 5 hours August 3 while crews worked to clear the wreckage from three separate crashes involving a total of four semi-trucks.
Source: http://www.wxii12.com/news/multiple-trucks-crash-on-i77-in-surry-county/41038874

13. *August 3, Victor Valley News* – (California) **Major crash involving semis shuts down 15 Freeway.** Southbound lanes of Interstate 15 in Mountain Pass, California, were closed for more than 3 hours August 3, while northbound lanes remained closed for about 7 hours after an accident involving 2 semi-trucks caused several 55-gallon drums of chlorine to leak on the roadway. One person was killed and HAZMAT crews worked to clean up the spill.
Source: http://www.vvng.com/major-crash-involving-semis-shuts-down-15-freeway/

Food and Agriculture Sector

14. *August 3, U.S. Department of Agriculture* – (National) **Grossglockner Inc., recalls pork products due to misbranding.** Grossglockner Inc., issued a recall August 3 for approximately 204 pounds of it “Handcrafted by Joseph Brunner Wegmans Bangers 8% Bread Crumbs” products sold in 16-ounce packages due to misbranding and

undeclared wheat after Wegmans Food Markets, Inc., store personnel discovered the products had an incorrect back label that did not declare the presence of wheat in the products. There have been no confirmed reports of adverse reactions and the products were distributed to Wegman's stores in Pennsylvania, Maryland, New Jersey, and Virginia.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-069-2016-release

15. *August 3, Food Safety News* – (National) **MI firm recalls 20,000 pounds of cheese linked to 7 E. coli illnesses.** Grassfields Cheese LLC issued a recall August 3 for approximately 20,000 pounds of its organic cheese products due to potential contamination with Shiga toxin-producing E.coli (STEC) after an E.coli outbreak that sickened 7 people between March and July 2016 was potentially linked to the company's cheese products. The affected products were sold at the firm's retail store in Michigan and via the company's Website nationwide.
Source: http://www.foodsafetynews.com/2016/08/130015/#.V6Mo1fkrKUk

Water and Wastewater Systems Sector

16. *August 3, WUSA 9 Washington, D.C.* – (Maryland) **Nearly 5 million gallons of sewage spilling into Patapsco River each day.** The Maryland Department of the Environment announced August 3 that a broken sewer line in Ellicott City is dumping nearly 5 million gallons of sewage per day into a portion of the Sucker Branch tributary of the Patapsco River following flash floods that hit the city July 30.
Source: http://www.wusa9.com/news/local/maryland/nearly-5-million-gallons-of-sewage-spilling-into-patapsco-river-each-day/286792677

17. *August 3, Associated Press* – (North Carolina) **Duke Energy says stormwater spilled from coal power plant.** Duke Energy officials reported August 3 that up to 50,000 gallons of storm water runoff spilled from their coal-fired power plant in Rutherford County, North Carolina, into the Broad River. Officials stated that while the water came into contact with unburned coal stored at the Rogers Energy Complex, it did not come into contact with any ash or harm the Broad River.
Source: http://www.wwaytv3.com/2016/08/03/duke-energy-says-stormwater-spilled-from-coal-power-plant/

Healthcare and Public Health Sector

18. *August 3, Reuters* – (National) **Banner Health says hackers may have gained access to patient data.** Banner Health notified approximately 3.7 million patients, health plan members, physicians, and health care providers August 3 of a potential data breach after hackers may have gained unauthorized access to patient, physician, and beneficiary data in computer systems that process card data at food and beverage outlets at Banner Health locations in 7 States between June 23 and July 7.
Source: http://www.reuters.com/article/us-bannerhealth-cyberattack-idUSKCN10E2RY

Government Facilities Sector

19. *August 3, KTVB 7 Boise* – (Idaho) **Pioneer Fire continues to threaten homes in Lowman.** Crews reached 36 percent containment August 3 of the more than 48,000-acre Pioneer Fire burning in the Boise National Forest in Idaho.
Source: http://www.ktvb.com/news/local/pioneer-fire-continues-to-threaten-homes-in-lowman/287280379

20. *August 3, Portland Oregonian* – (Oregon) **Rail fire grows to more than 5,500 acres, 10 homes on evacuation notice.** Crews worked August 2 to contain the 5,500-acre Rail Fire burning near Unity, Oregon, which has prompted about 10 homes to be put on an evacuation notice.
Source: http://www.oregonlive.com/pacific-northwest-news/index.ssf/2016/08/rail_fire_grews_to_more_than_5.html

21. *August 3, KUTV 2 Salt Lake City* – (Utah) **Box Elder County fire grows to 5,000 acres near Plymouth, Utah.** Crews worked August 3 to contain the 5,000-acre fire burning in Plymouth, Utah, which threatens 2 farms and a residential area.
Source: http://kutv.com/news/local/box-elder-county-fire-grows-to-5000-acres-near-portage-utah

22. *August 3, KTXL 40 Sacramento* – (California) **Cold Fire burns 4,600 acres in roughly 24 hours.** Crews reached 10 percent containment August 3 of the 4,600-acre Cold Fire burning near Winters, California.
Source: http://fox40.com/2016/08/03/cold-fire-burns-4600-acres-in-roughly-24-hours/

Emergency Services Sector

Nothing to report

Information Technology Sector

23. *August 4, SecurityWeek* – (International) **Critical flaws found in Cisco small business routers.** Cisco released patches for its small business RV series routers after researchers discovered a critical flaw affecting the Web interface that allows remote, unauthenticated attackers to execute arbitrary code with root privileges, a high severity flaw that can be exploited remotely to perform a directory traversal and access arbitrary files on the system, and a medium severity command shell injection flaw that could allow a local attacker to inject arbitrary shell commands that are then executed by the device, among other vulnerabilities.
Source: http://www.securityweek.com/critical-flaws-found-cisco-small-business-routers

24. *August 4, SecurityWeek* – (International) **Google patches 10 vulnerabilities in Chrome 52.** Google released an update for Chrome 52 resolving 10 security vulnerabilities after third-party developers discovered 4 high risk flaws affecting the Web browser including an address bar spoofing flaw, a use-after-free bug in Blink, and

heap overflow bugs in pdfium, as well as 3 medium risk bugs including a same origin bypass for imagines in Blink, and parameter sanitization failure bugs in DevTools.
Source: http://www.securityweek.com/google-patches-10-vulnerabilities-chrome-52

25. *August 3, Help Net Security* – (International) **Four high-profile vulnerabilities in HTTP/2 revealed.** Imperva released a report at the Black Hat USA 2016 conference documenting four high-profile vulnerabilities in Hypertext Transfer Protocol (HTTP)/2 after researchers from the Imperva Defense Center found a HPACK Bomb attack resembling a zip bomb, a dependency cycle attack that takes advantage of HTTP/2's flow control mechanisms for network optimization, stream multiplexing abuse that results in denial-of-service to legitimate users, and Slow Read attacks in server implementations from Apache, Microsoft, NGINX, Jetty, and nghttp2. The vendors of the HTTP/2 protocol mechanisms released patches for the issues.
Source: https://www.helpnetsecurity.com/2016/08/03/vulnerable-http2/

For another story, see item **2**

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

26. *August 4, WCBS 2 New York; Associated Press* – (New York) **Massive Queens warehouse fire under control.** New York Custom Interior Millwork Corporation in Queens, New York, was considered a total loss August 3 following a 5-alarm fire that prompted the response of over 250 firefighters. The cause of the fire remains under investigation.
Source: http://newyork.cbslocal.com/2016/08/04/queens-warehouse-fire-under-control/

27. *August 3, KTRK 13 Houston* – (Texas) **Three-alarm fire erupts at Galleria-area apartments.** Authorities are investigating the cause of a 3-alarm fire August 3 at the Courtyard Condominiums in Houston that damaged approximately 30 apartment units. No injuries were reported.
Source: http://abc13.com/news/firefighters-battling-3-alarm-fire-at-galleria-area-apartments/1455790/

28. *August 3, KOMO 4 Seattle* – (Washington) **25 residents run for their lives as flames gut Lynwood apartments.** About 25 residents were displaced from the Westwood Apartments August 3 following a fire that destroyed 4 apartment units and caused

significant damage to the roof.
Source: http://komonews.com/news/local/25-residents-run-for-their-lives-as-flames-gut-lynnwood-apartments

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