Daily Open Source Infrastructure Report
15 July 2016

Top Stories

- Severe thunderstorms that moved through Missouri and Illinois July 13 knocked out power to approximately 185,000 customers. – *St. Louis Post-Dispatch* (See item **1**)

- A fugitive pleaded guilty July 13 to defrauding around 800 investors out of an estimated $65 million in a Ponzi scheme where he and co-conspirators operated Cyprus Funds, Inc., to sell certificates of deposit and unregistered mutual funds in Latin America and the U.S. – *U.S. Attorney's Office, Northern District of Ohio* (See item **5**)

- A six-vehicle crash involving two semi-trucks and four other vehicles left one person dead, several others injured, and forced the closure of the westbound lanes of Interstate 84 in Montgomery, New York, for several hours July 13. – *Middletown Times Herald-Record* (See item **6**)

- A malfunctioning pumping station at the Amsterdam water treatment plant in New York caused over 500,000 gallons of sewage to leak into the Mohawk River July 13. – *WNYT 13 Albany* (See item **17**)

Fast Jump Menu

Energy Sector

1. *July 14, St. Louis Post-Dispatch* – (Missouri; Illinois) **No power for 100,000 in Missouri, Illinois after thunderstorms roar through area.** Severe thunderstorms that moved through Missouri and Illinois July 13 knocked out power to approximately 185,000 customers following strong winds that took down power lines.
Source: http://www.stltoday.com/news/local/metro/customers-without-power-as-thunderstorms-roar-across-st-louis-area/article_eda80e52-8d4a-5068-a250-d3fbe29ec316.html

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *July 14, St. Joseph-Benton Harbor Herald-Palladium* – (Michigan) **Cook plant's Unit 2 reactor back in operation.** The Unit 2 reactor at the Donald C. Cook Nuclear Generating Station in Bridgman, Michigan, was back online July 12 after it was shutdown July 6 when a rupture released steam and damaged the wall of the turbine building. Preliminary findings indicated that the steam line ruptured due to vibration-induced metal fatigue of a steam expansion joint bellows.
Source: http://www.heraldpalladium.com/news/local/cook-plant-s-unit-reactor-back-in-operation/article_8f76fcca-8b9f-52c7-9540-9dd7714ee77c.html

3. *July 14, Associated Press* – (North Carolina) **Pump motor sparks alert at Brunswick Nuclear Station.** Duke Energy Progress officials are investigating the cause of a damaged pump motor at its Brunswick Nuclear Generating Station near Southport, North Carolina, July 12 that prompted the company to reduce power in one of the plant's reactors to 70 percent and issue an alert.
Source: http://wnct.com/2016/07/13/pump-motor-sparks-alert-at-brunswick-nuclear-station/

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *July 13, Courier of Montgomery County* – (Texas) **Two arrested for credit card fraud scheme.** Two individuals were arrested and charged in Montgomery County, Texas, July 11 after authorities discovered approximately 100 stolen credit cards and a credit card embossing machine, among other illicit material in the duo's vehicle during

a routine traffic stop.
Source: http://www.yourhoustonnews.com/courier/news/two-arrested-for-credit-card-fraud-scheme/article_40ce2d27-4b12-53fc-8b70-508008f101e4.html

5. *July 13, U.S. Attorney's Office, Northern District of Ohio* – (International) **Longtime fugitive pleads guilty to stealing $65 million from hundreds of people.** A fugitive, initially indicted in October 2003 pleaded guilty July 13 to defrauding around 800 investors out of an estimated $65 million in a Ponzi scheme where he and co-conspirators operated Doylestown, Ohio-based Cyprus Funds, Inc., to sell certificates of deposit and unregistered mutual funds in Latin America and the U.S. from 1995 – 1999.
Source: https://www.justice.gov/usao-ndoh/pr/longtime-fugitive-eric-bartoli-pleads-guilty-stealing-65-million-hundreds-people

Transportation Systems Sector

6. *July 14, Middletown Times Herald-Record* – (New York) **Police: One person dead, multiple injuries in six-vehicle crash on I-84.** A six-vehicle crash involving two semi-trucks and four other vehicles left one person dead, several others injured, and forced the closure of the westbound lanes of Interstate 84 in Montgomery, New York, for several hours July 13.
Source: http://www.recordonline.com/news/20160713/police-one-person-dead-multiple-injuries-in-six-vehicle-crash-on-i-84

7. *July 14, KGW 8 Portland* – (Oregon) **Two people killed after trucks collide on Highway 47.** A 2-vehicle crash left 2 people dead and closed Highway 47 at the junction with Highway 26 in Vernonia for several hours July 13.
Source: http://www.kgw.com/news/local/washington-county/two-people-killed-in-highway-47-crash/272155861

8. *July 13, San Francisco Bay City News* – (California) **CHP officer injured in crash near American Canyon while responding to I-80 pursuit.** The eastbound lanes of Highway 80 in Solano County were closed for nearly 3 hours July 13 after a California Highway Patrol officer crashed his motorcycle during a pursuit. The officer was transported to an area hospital with minor injuries.
Source: http://abc7news.com/traffic/chp-officer-injured-in-crash-near-american-canyon-while-responding-to-i-80-pursuit/1425793/

9. *July 13, Duluth News Tribune* – (Minnesota; Wisconsin) **List of flood-related road closures in the Northland.** Severe flooding prompted the closure of several highways and roads throughout Minnesota and Wisconsin July 12 until the water recedes.
Source: http://www.duluthnewstribune.com/news/4072496-list-flood-related-road-closures-northland

10. *July 13, Redding Record Searchlight* – (California) **United Express flight returns to Redding after landing-gear malfunction.** A United Express flight en route to San Francisco from Redding was forced to make an emergency landing at Redding

Municipal Airport shortly after takeoff after its landing gear failed to retract July 13. The plane landed safely and crews are inspecting the jet to determine what caused the malfunction.
Source: http://www.redding.com/news/local/United-Express-flight-makes-has-returns-to-Redding-after-landing-gear-malfunction-386699271.html

Food and Agriculture Sector

11. *July 14, U.S. Department of Agriculture* – (National) **Michael Angelo's Gourmet Foods, Inc. recalls shrimp scampi products due to misbranding and undeclared allergens.** Michael Angelo's Gourmet Foods, Inc., issued a recall July 13 for approximately 4,225 pounds of its "Michael Angelo's Uncompromisingly Italian-Style Shrimp Scampi with Linguini Pasta in a Fresh Heirloom Garlic-Butter Sauce" products sold in 26-ounce packages due to misbranding and undeclared chicken, soy, and egg after the company received a customer complaint stating that the packages contain a chicken piccata product due to a packaging error. There have been no confirmed reports of adverse reactions and the products were shipped to distributors in the southeastern U.S.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-059-2016-release

12. *July 13, U.S. Food and Drug Administration* – (International) **Kerry Inc. recalls Golden Dipt Jalapeno Breaders because of possible health risk** Kerry Inc., issued a recall July 12 for two lots of its Golden Dipt Jalapeno Breader products due to potential E.coli O121 contamination after one of the company's suppliers notified the firm that two of their ingredients used in the products, a red bell pepper nugget and a jalapeno nugget, were made with flour recalled by General Mills, Inc., due to potential E.coli O121 contamination. No illnesses have been reported and the products were sold to foodservice distributors in seven States and in Canada.
Source: http://www.fda.gov/Safety/Recalls/ucm510986.htm

13. *July 13, U.S. Food and Drug Administration* – (National) **Baptista's Bakery issues allergy alert on undeclared milk in Snack Factory Original Pretzel Crisps.** Baptista's Bakery, Inc., issued a voluntary recall July 12 for a limited quantity of its Snack Factory Original Pretzel Crisps sold in 30-ounce packages due to mislabeling and undeclared milk ingredients after it was discovered that the pretzel crisps were produced in the same facility as seasoned products containing milk and may have come in contact with milk ingredients. No illnesses have been reported.
Source: http://www.fda.gov/Safety/Recalls/ucm510965.htm

14. *July 13, U.S. Food and Drug Administration* – (National) **International Commissary Corporation issues voluntary recall of Marie Callender's Cheese Biscuit Mix due to possible health risk.** International Commissary Corporation (ICC) issued a voluntary recall July 13 for select lots of its Marie Callender's Cheese Biscuit Mix sold in 7-ounce and 14-ounce packages due to potential E.coli O121 contamination after ICC was notified by its supplier that an ingredient used in the mixes contains flour recalled by General Mills, Inc. No illnesses have been reported and the products were

sold in retail stores in five States.
Source: http://www.fda.gov/Safety/Recalls/ucm511104.htm

15. *July 13, U.S. Food and Drug Administration* – (National) **IKEA N.A. Services, LLC voluntary issues expanded recall and allergy alert on undeclared milk, almond, and/or hazelnut on certain IKEA chocolate products** IKEA North America Services, LLC expanded a previous recall July 6 for select lots of its chocolate products sold in seven variations due to misbranding and undeclared milk, hazelnuts, and/or almonds after sample analysis of the chocolate revealed that the products contained the undeclared ingredients. No illnesses have been reported and the products were distributed to IKEA retail stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm510979.htm

Water and Wastewater Systems Sector

16. *July 14, CNN* – (Ohio) **Ohio town water manager charged over lead contamination.** Officials announced that the former water system operator in Sebring, Ohio, was charged July 13 for violating State safe drinking water laws by failing to notify residents of high lead levels in their tap water immediately after a lab confirmed the high levels in samples taken during routine tap water testing in August and September 2015.
Source: http://www.cnn.com/2016/07/14/us/ohio-lead-contaminated-water-charges/

17. *July 13, WNYT 13 Albany* – (New York) **500,000 gallons of sewage spill into Mohawk River.** The New York State Department of Environmental Conservation announced July 13 that a malfunctioning pumping station at the Amsterdam water treatment plant in New York caused over 500,000 gallons of sewage to leak into the Mohawk River. Officials stated that drinking water was not impacted by the spill.
Source: http://wnyt.com/news/mohawk-river-sewage-spill-amsterdam/4198329/

Healthcare and Public Health Sector

Nothing to report

Government Facilities Sector

18. *July 14, KUSA 9 Denver* – (Colorado) **Hayden Pass Fire prompts new evacuations.** Crews worked July 14 to contain the nearly 13,000-acre Hayden Pass Fire burning southeast of Salida. The Fremont County Sheriff's Office stated that County Road 35 and the Eagle Peak Subdivision on the west side of County Road 1A were under mandatory evacuation orders.
Source: http://www.9news.com/news/local/wildfires/hayden-pass-fire-grows-600-acres/271953864

19. *July 14, WTKR 3 Norfolk* – (Virginia) **Four treated, three taken to hospital after chemical leak at College of William & Mary.** Four people were treated and three were taken to an area hospital July 13 after an unknown amount of people were

exposed to a chemical from a broken pipe at Zable Stadium at the College of William & Mary in Williamsburg. The construction site at the stadium was evacuated while crews contained the leak.
Source: http://wtkr.com/2016/07/13/four-treated-three-taken-to-hospital-after-chemical-leak-at-college-of-william-mary/

20. *July 13, Salt Lake Tribune* – (Utah) **Utah's Saddle Fire continues to burn with 52 percent containment.** Crews reached 52 percent containment July 13 of the 2,296-acre Saddle Fire burning in Washington County, Utah. Officials estimated that the fire will be contained by August 1.
Source: http://www.sltrib.com/home/4112734-155/utahs-saddle-fire-continues-to-burn

Emergency Services Sector

21. *July 14, Omaha World-Herald* – (Nebraska) **6th inmate charged in deadly 2015 riot at Tecumseh State Prison.** A sixth inmate was charged July 13 for his role in a May 2015 riot at the Tecumseh State Prison in Nebraska that left two inmates dead and the facility extensively damaged. The inmate was charged with arson in connection to four separate fires that were set during the incident.
Source: http://www.omaha.com/news/crime/th-inmate-charged-in-deadly-riot-at-tecumseh-state-prison/article_82bcf123-ddee-5c38-8bb3-4196bbd29e11.html

Information Technology Sector

22. *July 14, IDG News Service* – (International) **Juniper patches high-risk flaws in Junos OS.** Juniper Networks fixed several vulnerabilities in the Junos operating system (OS) used on its networking and security appliances, including an information leak in the J-Web interface, vulnerabilities that could lead to denial of service conditions, a potential kernel crash, a potential memory buffer (mbuf) leak, a crypto vulnerability, and an issue with SRX Series devices.
Source: http://www.networkworld.com/article/3095812/juniper-patches-high-risk-flaws-in-junos-os.html

23. *July 14, Softpedia* – (International) **Microsoft discovers new version of Troldesh ransomware.** Microsoft Malware Protection Center researchers discovered a new version of the Troldesh ransomware, also known as Encoder.858 and Shade Ransomware, that contains new modifications including a dedicated payment portal where users can get information on how to pay the ransom, utilization of a Tor Web site, and two new extensions, ".da_vinci_code" and ".magic_software_syndicate," which are added to the end of encrypted files.
Source: http://news.softpedia.com/news/microsoft-discovers-new-version-of-troldesh-ransomware-506321.shtml

24. *July 14, Softpedia* – (International) **Huge spam wave drops Locky variant that can work without an internet connection.** F-Secure researchers examined a July 12 campaign utilizing the Locky ransomware where the group sent out 120,000 spam email messages every 2 hours in 2 instances of activity. Avira researchers also found

that a new Locky variant works in "offline mode," making it harder to block.
Source: http://news.softpedia.com/news/huge-spam-wave-drops-locky-variant-that-can-work-without-an-internet-connection-506294.shtml

25. *July 13, IDG News Service* – (International) **Three popular Drupal modules patch site-takeover flaws.** Drupal, a content management system, worked with three third-party module maintainers, RESTWS, Coder, or Webform Multiple File Upload, to address critical vulnerabilities that could allow attackers to take control of Web sites, including a flaw that allows attackers to execute rogue Hypertext Preprocessor (PHP) code Web servers that host Drupal Web sites with the modules, as well as flaws that could lead to remote code execution (RCE).
Source: http://www.computerworld.com/article/3095388/security/three-popular-drupal-modules-patch-site-takeover-flaws.html

26. *July 13, Softpedia* – (International) **Ransomware permanently deletes your files then has the nerve to ask for money.** Cisco Talos researchers discovered a new piece of ransomware dubbed Ranscam that deletes the victim's files after infecting the computer, and removes core Microsoft Windows executables responsible for the System Restore feature, hard drive shadow copies, and several registry keys associated with booting into Safe Mode, among other modifications. Once the removal is complete, the ransomware shows its ransom note and falsely informs the victim that their files are encrypted and moved into a hidden partition.
Source: http://news.softpedia.com/news/ransomware-permanently-deletes-your-files-then-has-the-nerve-to-ask-for-money-506289.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

27. *July 14, WUSA 9 Washington, D.C.* – (Maryland) **Six Flags re-opens after bomb threat.** The Six Flags America amusement park in Prince George's County was closed for nearly 5 hours July 13 following a phoned bomb threat and the discovery of two suspicious backpacks. Police cleared the scene after determining that there was no threat.
Source: http://www.wusa9.com/news/local/maryland/bomb-threat-reported-at-six-flags-america/271899888

28. *July 13, KATU 2 Portland* – (Oregon) **3-alarm shop fire ignites natural gas leak in**

Perrydale. A Perrydale, Oregon business housing antique vehicles and farm equipment was deemed a total loss July 13 following a three-alarm fire that caused a natural gas leak in the building to ignite. Officials shut off the gas line and repaired the leak and the cause of the fire remains under investigation.
Source: http://katu.com/news/local/3-alarm-commercial-shop-natural-gas-fire-in-perrydale-amity

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.