Daily Open Source Infrastructure Report
09 August 2016

Top Stories

- Federal officials approved a $32 million project August 6 permitting Eastern Shore Natural Gas to build new compression facilities, extend natural gas lines, and install more than 10 miles of underground pipes in Delaware. – *New Castle County News Journal* (See item **1**)
- Eighteen former Midwest Bank officers and directors agreed to pay $26.5 million to the Federal Deposit Insurance Corporation August 5 to settle charges alleging that their negligent lending practices from 2005 – 2008 caused the bank over $128 million in losses. – *Chicago Tribune* (See item **2**)
- The Hawaii Department of Environmental Services (ENV) reported August 5 that approximately 12,950 gallons of sewage overflowed near the University of Hawaii at Manoa. – *KHON 2 Honolulu* (See item **18**)
- A former office manager at a dentist's office in White Plains, New York, was charged August 4 after she allegedly embezzled over $500,000 from the business from December 2007 – March 2015. – *Lower Hudson Valley Journal News* (See item **19**)

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. *August 6, New Castle County News Journal* – (Delaware) **$36M gas pipeline project in Del. wins federal approval.** Federal officials approved a $32 million pipeline project August 6 that permits Eastern Shore Natural Gas to extend natural gas transmission lines, install more than 10 miles of underground pipelines, and build new compression facilities in New Castle and Kent counties in Delaware, among other plans in an effort to strengthen its transmission infrastructure. The project will begin in September 2016 and is expected to be completed in 2017.
   Source: http://www.delawareonline.com/story/money/business/delawareinc/2016/08/06/36m-gas-pipeline-project-del-wins-federal-approval/88332416/

For another story, see item **9**

Chemical Industry Sector

Nothing to report

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

2. *August 5, Chicago Tribune* – (Illinois) **Midwest Bank officials, FDIC in settlement for $26.5 million over loans.** The Federal Deposit Insurance Corporation announced August 5 that 18 former Midwest Bank officers and directors agreed to pay a total of $26.5 million to settle charges alleging that the officers' negligence in lending over $100 million to 6 risky borrowers from 2005 – 2008 without properly analyzing the borrowers' creditworthiness caused the bank over $128 million in losses.
   Source: http://www.chicagotribune.com/business/ct-midwest-bank-settlement-0805-biz-20160804-story.html

3. *August 5, SecurityWeek* – (International) **New ATM hacking method uses stolen EMV card data.** Rapid7 researchers discovered that Europay, Mastercard, and Visa (EMV) cards are susceptible to fraudulent transactions after finding that an attacker could insert a shimming device into the card slot of a point-of-sale (PoS) system to intercept and capture card data, which is then remotely sent to another device, dubbed

"La-Cara." La-Cara feeds the stolen transaction data to the targeted ATM, thereby allowing the fraudsters to withdraw up to $50,000 from the victim's card.
Source: http://www.securityweek.com/new-atm-hacking-method-uses-stolen-emv-card-data

Transportation Systems Sector

4. *August 8, KOLO 8 Reno* – (Nevada) **Five hurt in rollover on Mt. Rose Highway.** The eastbound lane of Mt. Rose Highway in Reno, Nevada, was closed for nearly 4 hours August 7 while crews worked to recover a vehicle that veered off the road and fell into a 40-foot embankment, leaving 5 people injured.
Source: http://www.kolotv.com/content/news/Rollover-accident-leaves--389448851.html

5. *August 8, NBC News* – (International) **Delta warns of chaos after power outage, worldwide system failure.** A power outage at the Delta Airlines headquarters in Atlanta August 8 caused a global computer failure that forced the cancellation of at least 451 flights and left less than 1,700 of the company's 6,000 scheduled flights in operation. The outage affected check-in systems, airport screens, as well as the airline Website and smartphone apps for more than 6 hours.
Source: http://www.nbcnews.com/business/travel/delta-system-outage-triggers-delays-worldwide-n625141

6. *August 7, West Central Tribune* – (Minnesota) **U.S. Highway 12 accident disrupts traffic, power in east Willmar.** A single-vehicle rollover crash shut down U.S. Highway 12 in east Willmar, Minnesota, for several hours August 7 and knocked out power to various parts of Willmar after the vehicle struck a power pole next to the roadway.
Source: http://www.wctrib.com/news/local/4089795-us-highway-12-accident-disrupts-traffic-power-east-willmar

7. *August 7, WKRG 5 Mobile*– (Alabama) **Deadly crash on Highway 45 Saturday Afternoon.** U.S. Highway 45 near Mobile, Alabama, was closed for several hours August 6 while crews worked to clear the wreckage from a fatal two-vehicle crash that left two people dead and four others injured.
Source: http://wkrg.com/2016/08/07/deadly-crash-on-highway-45-saturday-afternoon/

8. *August 6, Riverhead News-Review* – (New York) **Driver in crash charged with DWAI.** Eastbound Sunrise Highway in East Hampton, New York, was closed for approximately 4 hours August 6 while officials investigated the scene of a single-vehicle crash after a vehicle crashed into two pedestrians. The driver and both pedestrians were transported to area hospitals with injuries.
Source: https://riverheadnewsreview.timesreview.com/2016/08/75499/two-pedestrians-hit-on-sunrise-highway-in-flanders/

9. *August 6, KTVT 11 Fort Worth* – (Texas) **Thousands of gallons of fuel spilled after tanker crash.** HAZMAT crews worked for several hours August 6 to clean up after a

tanker truck overturned on Trinity Boulevard in Fort Worth, Texas, spilling about 2,000 gallons of diesel fuel onto the roadway and into a nearby creek. The driver and a firefighter were transported to area hospitals with injuries.
Source: http://dfw.cbslocal.com/2016/08/06/thousands-of-gallons-of-fuel-spilled-after-tanker-crash/

10. *August 6, Columbia State* – (South Carolina) **3 people killed Saturday in separate crashes on I-20 identified.** Interstate 20 in Columbia, South Carolina, was closed for more than 6 hours August 6 while crews worked to clear the wreckage following two unrelated crashes that left a total of three people dead.
Source: http://www.thestate.com/news/local/article94108807.html

11. *August 6, WJDT 58 Milwaukee* – (Wisconsin) **Mukwonago motorcyclist dies in late night crash.** A three-vehicle crash involving two motorcycles and another vehicle prompted the closure of County Highway NN near Eagle, Wisconsin, for several hours August 5 – August 6 while Waukesha County officials investigated the scene. One person was killed and two others were transported to an area hospital with injuries.
Source: http://www.cbs58.com/story/32699609/mukwonago-motorcyclist-dies-in-late-night-crash

12. *August 5, WBRZ 2 Baton Rouge*– (Louisiana) **I-10 reopened after crews remove overturned tanker.** Interstate 10 East in Baton Rouge, Louisiana, was closed for several hours August 5 while crews worked to clear the wreckage after a semi-truck overturned when it collided with another vehicle that ran off the roadway. The semi-truck driver was taken to an area hospital with minor injuries and authorities are searching for the other driver who fled on foot after the crash.
Source: http://www.wbrz.com/news/overturned-18-wheeler-closes-i-10-east-past-siegen-lane-and-i-10-12-split/

For another story, see item **1**

Food and Agriculture Sector

13. *August 8, U.S. Food and Drug Administration* – (National) **Gel Spice, Inc., issues expanded recall of ground turmeric powder due to elevated lead levels.** Gel Spice, Inc., expanded a previous recall August 5 for its ground turmeric powder products sold under seven brands after sampling and testing revealed elevated levels of lead in a product produced from the same bulk turmeric as the ground turmeric powder products. No illnesses have been reported and the products were distributed to retailers nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm515328.htm

14. *August 7, U.S. Department of Agriculture* – (National) **Al Shabrawy Meat Incorporated recalls meat and poultry products due to misbranding and undeclared allergens.** Al Shabrawy Meat Inc., issued a recall August 6 for its meat and poultry products sold in nine variations due to misbranding and undeclared pistachio nut and soy discovered during an on-going investigation at the company's

South River, New Jersey facility. There have been no confirmed reports of adverse reactions and the products were shipped to retail locations and wholesalers in six States.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-070-2016-release

15. *August 6, U.S. Food and Drug Administration* – (National) **Beyond Better Foods, LLC issues allergy alert on undeclared peanuts in mislabeled Peanut Butter Chocolate Chip ice cream.** Beyond Better Foods, LLC issued a recall August 6 for select lots of its Enlightened brand Peanut Butter Chocolate Chip ice cream products due to mislabeling and undeclared peanuts after it was discovered the products may have been packaged in Mint Chocolate Chip ice cream containers. No illnesses have been reported and the products were distributed to retail stores nationwide.
Source: http://www.fda.gov/Safety/Recalls/ucm515304.htm

16. *August 5, CNN* – (National) **Salmonella outbreak in 9 states linked to alfalfa sprouts.** The U.S. Centers for Disease Control and Prevention and U.S. Food and Drug Administration are investigating August 5 after a Salmonella outbreak that has sickened 30 people across 9 States since May was potentially linked to alfalfa sprouts supplied by Denver-based Sprouts Extraordinaire. Sprouts Extraordinaire issued a recall August 5 for its "Living Alfalfa Sprouts" products sold in 5-pound packages as a result of the Salmonella outbreak.
Source: http://www.cnn.com/2016/08/05/health/salmonella-outbreak-alfalfa-sprouts/

For another story, see item **33**

Water and Wastewater Systems Sector

17. *August 7, KAAL 6 Austin* – (Minnesota) **Officials: 3,500 gallons of lake water and contamination removed; lake and park still closed.** The Minnesota Pollution Control Agency (PCA) worked August 7 to remove approximately 3,500 gallons of lake water and sewage after approximately nearly 5,000 gallons of sewage spilled into the Beaver Lake August 6, prompting the closure of the Beaver Lake County Park. The type and source of the contamination remain under investigation and crews are working to clear the remaining contaminate.
Source: http://www.kaaltv.com/news/sewage-spill-steele-county-beaver-lake-dam-mn-dnr-mn-pca-residents-homeowners-park-closed/4225703/

18. *August 6, KHON 2 Honolulu*– (Hawaii) **Nearly 13,000 gallons of sewage spill in University area.** Officials from the Hawaii Department of Environmental Services (ENV) reported August 5 that approximately 12,950 gallons of sewage overflowed near the University of Hawaii at Manoa after debris that entered a storm drain caused blockage. Crews released the blockage, cleaned the area, and advised swimmers to avoid Magic Island and the Ala Wai Boat Harbor.
Source: http://khon2.com/2016/08/06/nearly-13000-gallons-of-sewage-spill-in-university-area/

Healthcare and Public Health Sector

19. *August 6, Lower Hudson Valley Journal News* – (New York) **Mohegan Lake woman stole $500K from employer, police say.** A former office manager at Advanced Periodontics and Implant Dentistry of Westchester in White Plains, New York, was charged August 4 after she allegedly embezzled over $500,000 from the business by opening an unauthorized business credit card to pay for her personal expenses from December 2007 – March 2015.
    Source: http://www.lohud.com/story/news/crime/2016/08/06/mohegan-lake-woman-stole-employer/88325462/

20. *August 5, U.S. Food and Drug Administration* – (National) **Hospira issues a voluntary nationwide recall for one lot of 0.25% Bupivacaine Hydrochloride Injection, USP due to the presence of particulate matter within a single vial.** Hopsira, Inc., issued a voluntary recall August 5 for one lot of its 0.25% Bupivacaine Hydrochloride Injection products due to the presence of particulate matter after the company received a complaint stating particulate matter was found in one vial. No illnesses or adverse reactions have been reported and the products were distributed to wholesalers and hospitals nationwide.
    Source: http://www.fda.gov/Safety/Recalls/ucm515199.htm

Government Facilities Sector

21. *August 8, KTTV 11 Los Angeles* – (California) **'Pilot Fire' burning near Silverwood Lake grows to 4,500 acres.** Crews worked August 7 to contain the 4,500-acre Pilot Fire burning in the San Bernardino National Forest in California which has prompted evacuation orders for the Summit Valley area east of Cedar Springs Dam and forced the closure of Highway 173 between Highway 138 and Arrowhead Lake Road.
    Source: http://www.foxla.com/news/local-news/186308761-story

22. *August 7, KVAL 13 Eugene* – (Oregon) **Bybee Creek Fire containment increases, evacuation notice lifted.** Crews reached 59 percent containment August 7 of the 1,072-acre Bybee Creek Fire burning near Crater Lake National Park in Oregon, prompting officials to lift evacuation notices for Rim Village and park headquarters.
    Source: http://kval.com/news/local/bybee-creek-fire-containment-increases-evacuation-notice-lifted

23. *August 6, KCPQ 13 Tacoma* – (Washington) **Mandatory evacuations for Smyrna, Lower Crab Creek fire grows to 10,000 acres.** Officials issued mandatory evacuation orders for the Smyrna community and closed Lower Crab Creek Road from Smyrna to Beverly August 6 while crews worked to contain the more than 10,000-acre Lower Crab Creek Fire burning near Smyrna, Washington.
    Source: http://q13fox.com/2016/08/06/mandatory-evacuations-for-smyrna-community-due-to-a-wildfire/

24. *August 6, KBOI 2 Boise* – (Idaho) **Level 2 evacuations issued in Lowman, Pioneer fire burns 58,136 acres.** Officials issued an evacuation advisory August 6 in response

to the 58,136-acre Pioneer Fire burning near Lowman, Idaho, which has prompted the closure of Highway 21 and Banks-Lowman Road between Pine Flats and Lowman.
Source: http://kboi2.com/news/local/pioneer-fire-is-up-to-58136-acres-20-percent-containment

25. *August 5, Salt Lake Tribune* – (Utah) **Broad Mouth Fire nears 21,000 acres in Box Elder County.** Crews reached 30 percent containment August 5 of the 20,614-acre Broad Mouth Fire burning in Box Elder County, Utah.
Source: http://www.sltrib.com/news/4199113-155/broad-mouth-fire-nears-21000-acres

26. *August 5, Libby Western News* – (Montana) **Copper King Fire near T. Falls grows to 1,286 acres.** Crews worked August 5 to contain the 1,286-acre Copper King Fire burning near Thompson Falls, Montana, which has caused an estimated $1.3 million in damage.
Source: http://www.thewesternnews.com/news/copper-king-fire-near-t-falls-grows-to-acres/article_6d2c9e44-5b2c-11e6-a2be-a3d9160a32fd.html

Emergency Services Sector

Nothing to report

Information Technology Sector

27. *August 8, Help Net Security* – (International) **Remote Butler attack; APT groups' dream come true.** Microsoft security researchers developed an extension of the "Evil Maid" attack dubbed "Remote Butler" which allows attackers to bypass local Windows authentication to defeat full disk encryption without physical access to the targeted device. A patch released by Microsoft for the "Evil Maid" attack also prevents attackers from carrying out a "Remote Butler" attack.
Source: https://www.helpnetsecurity.com/2016/08/08/remote-butler-attack/

28. *August 6, Softpedia* – (International) **Cerber ransomware v2 spotted online, is now undecryptable.** Trend Micro researcher PanicAll discovered that the Cerber ransomware was updated in versions v1.5 and v2 to break a previous decryption tool that allowed users to recover their hacked files for free. The updates changed the extension added at the end of each encrypted file from ".cerber" to ".cerber2," and extended encryption keys generated by CryptGenRandom Microsoft application programming interface (API) from 16 bytes to 32 bytes, among other updates.
Source: http://news.softpedia.com/news/cerber-ransomware-v2-spotted-online-is-now-undecryptable-507045.shtml

29. *August 6, Softpedia* – (International) **Linux botnets dominate the DDoS landscape.** Kaspersky Lab released its distributed denial-of-service (DDoS) Intelligence Report which reported that Linux botnets accounted for 70.2 percent of all DDoS attacks initiated during quarter 2 (Q2) of 2016, while only 44.5 percent of DDoS attacks were carried out by Linux botnets in quarter 1. The report also stated that SYN DDoS attacks were the most popular methods for DDoS attacks during Q2, followed by transmission

control protocol (TCP), Hypertext Transfer Protocol Secure (HTTP), and Internet control message protocol (ICMP) floods.
Source: http://news.softpedia.com/news/linux-botnets-dominate-the-ddos-landscape-507043.shtml

30. *August 5, Softpedia* – (International) **New Remcos RAT available for purchase on underground hacking forums.** Symnatec researchers reported that a malware developer dubbed Viotto posted the Remcos Remote Access Trojan (RAT) targeting Microsoft Windows versions XP and higher for sale on underground hacking forums, which allows hackers the ability to take screenshots of infected computers, log keystrokes offline or in real times, and record content via the infected device's camera, among other malicious actions, and send the stolen data encrypted via Hypertext Transfer Protocol Secure (HTTPS) to the command and control (C&C) server. Researchers also discovered the trojan can queue operations to be carried out when the victim goes online and includes a password dumping component that can dump passwords from applications like Microsoft's Internet Explorer, Mozilla Firefox, and Apple Inc.'s Safari, among others.
Source: http://news.softpedia.com/news/new-remcos-rat-available-for-sale-on-underground-hacking-forums-507018.shtml

31. *August 5, SecurityWeek* – (International) **VMware Tools flaw allowed code execution via DLL hijacking.** VMware published an advisory describing two vulnerabilities in several of its products including a dynamic-link library (DLL) hijacking issue in the Windows version of VMware Tools related to the VMware Host Guest Client Redirector component that could be exploited to execute arbitrary code on a targeted system after finding that when a document is opened from a uniform naming convention (UNC) path, the Client Redirector injects a DLL named "vmhgfs.dll" into the file in order to open the file, allowing an attacker to load a malicious DLL into the application and to compromise the system. The second vulnerability is a Hypertext Transfer Protocol Secure (HTTP) header injection issue in vCenter Server and ESXi caused by a lack of input validation that could allow a hacker to launch cross-site scripting (XSS) or malicious redirect attacks.
Source: http://www.securityweek.com/vmware-tools-flaw-allowed-code-execution-dll-hijacking

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

See item 5

Commercial Facilities Sector

32. *August 6, KOIN 6 Portland* – (Oregon) **4 bodies found in rubble of Newport motel after fire.** Authorities are investigating the cause of an August 5 fire at the Newport City Center Motel in Newport, Oregon, that caused significant damage to the motel, left 50 people displaced, killed 4, and injured 3 others.
Source: http://koin.com/2016/08/05/fire-burning-at-newport-city-center-motel/

33. *August 6, WMUR 9 Manchester* – (New Hampshire) **Crews battle 4-alarm blaze at lumber distributor in Kingston.** Authorities are investigating the cause of a four-alarm fire at Northland Forest Products in Kingston, New Hampshire, that caused an estimated millions of dollars in damage and injured one firefighter.
Source: http://www.wmur.com/news/crews-battle-4alarm-blaze-at-lumber-distributor-in-kingston/41079622

Dams Sector

Nothing to report

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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.