Daily Open Source Infrastructure Report
17 September 2015

Top Stories

- A September 15 rain storm in California prompted 100 residents to evacuate, left 10,000 customers without power overnight, and caused all lanes of 710 Freeway to shut down. – *KTLA 5 Los Angeles* (See item **7**)

- Residents in Utah and Arizona were issued boil water advisory September 14 due to a flash flood that damaged and killed 16 people and injured several others. – *CNN* (See item **18**)

- A Los Angeles-based surgeon was charged in an indictment unsealed September 15 for working with 14 associates to bilk insurance companies out of $150 million through unnecessary operations performed by untrained staff. – *Associated Press* (See item **20**)

- A Russian national pleaded guilty September 15 to leading a hacking and data breach scheme that compromised the Nasdaq stock market and payment systems at several companies, resulting in losses of over $300 million between 2005 and 2012. – *Agence France-Presse* – (See item **35**)

Fast Jump Menu

PRODUCTION INDUSTRIES	SERVICE INDUSTRIES
• Energy	• Financial Services
• Chemical	• Transportation Systems
• Nuclear Reactors, Materials, and Waste	• Information Technology
• Critical Manufacturing	• Communications
• Defense Industrial Base	• Commercial Facilities
• Dams	**FEDERAL and STATE**
SUSTENANCE and HEALTH	• Government Facilities
• Food and Agriculture	• Emergency Services
• Water and Wastewater Systems	
• Healthcare and Public Health	

Energy Sector

1. *September 16, Associated Press* – (National) **Feds backlogged on well inspections.** An official with the U.S. Department of Interior announced September 15 that the Bureau of Land Management has an extensive backlog of inspections for high-risk oil and gas wells on Federal land and lacks sufficient resources to conduct the inspections while a drilling boom continues across several States.
Source: http://triblive.com/business/headlines/9097507-74/gas-jewell-federal

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *September 16, WWJ 62 Detroit; Associated Press* – (Michigan) **Fermi 2 nuclear power plant shuts down for evaluation, possible repairs.** DTE Energy Co., reported that the reactor at the Fermi 2 nuclear power plant in Frenchtown has been shut down September 13 due to a problem with a system used to cool auxiliary equipment. Crews plan to evaluate plant equipment and to see if repairs are necessary.
Source: http://detroit.cbslocal.com/2015/09/16/fermi-2-nuclear-power-plant-shuts-down-for-evaluation-possible-repairs/

3. *September 16, Associated Press* – (Arizona) **Responders holding Palo Verde response exercise.** Emergency officials held a daylong preparedness exercise September 16 that involved more than 400 State, local, and tribal agencies for a mock incident at Palo Verde Nuclear Generation Station west of Phoenix. The exercise is designed to ensure emergency facilities and a joint information center can activate quickly.
Source: http://www.mysanantonio.com/business/energy/article/Responders-holding-Palo-Verde-response-exercise-6507933.php

Critical Manufacturing Sector

4. *September 14, U.S. Department of Labor* – (Texas) **OSHA cites El Paso stamping plant for amputations and other serious safety hazards.** The Occupational Safety and Health Administration issued Stampcoat Inc., doing business as El Paso Tool & Die 33 citations September 14 for health and safety violations including failing to properly safeguard workers against caught-between and impact hazards, failing to properly shut down machinery during servicing and maintenance, and failing to train workers on personal protective equipment, among other violations after an inspection following two incidents where workers had their fingers crushed or sheared off. Proposed penalties total $119,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=28701

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

5. *September 15, U.S. Attorney's Office Southern District of New York* – (National) **Two defendants plead guilty in Manhattan federal court for their roles in orchestrating $18.5 million mortgage modification fraud scheme.** Two men pleaded guilty September 15 for their roles in a mortgage modification scheme which defrauded over 8,000 homeowners out of more than $18.5 million by charging homeowners exorbitant fees for promised mortgage modifications that were never provided.
Source: http://www.justice.gov/usao-sdny/pr/two-defendants-plead-guilty-manhattan-federal-court-their-roles-orchestrating-185

6. *September 15, Reuters* – (International) **RBS in $129.6 mln mortgage securities deal with U.S. regulator.** The Royal Bank of Scotland Group PLC (RBS) agreed September 15 to pay $129.6 million to the National Credit Union Administration to resolve allegations that RBS ignored underwriting guidelines and sold toxic mortgage-backed securities to now-failed credit unions.
Source: http://www.reuters.com/article/2015/09/15/rbs-settlement-mbs-idUSL1N11L2R020150915

For additional stories, see items **20** and **35**

Transportation Systems Sector

7. *September 16, KTLA 5 Los Angeles* – (California) **Record rainfall wreaks havoc on SoCal roads, prompting evacuations and leaving thousands without power.** A September 15 rain storm in Southern California prompted 100 residents to evacuate from an assisted living facility, left 10,000 Department of Water and Power customers without power overnight, and caused all lanes of 710 Freeway in Bell, California, to shut down after up to two-inches of rain flooded Los Angeles County. Several SigAlerts were issued after multiple collisions occurred.
Source: http://ktla.com/2015/09/15/rain-moves-into-southern-california-overnight-flood-advisory-issued-in-parts-of-l-a-county/

8. *September 16, CNN* – (Alaska) **Alaska plane crashed kills 3 people; 7 survivors reported.** An Alaska Air National Guard official reported September 16 that a small plane crashed near Iliamna Airport, killing 3 people and injuring 7 others September 15. The National Transportation Safety Board is investigating the cause of the accident.
Source: http://www.cnn.com/2015/09/15/us/alaska-plane-crash/index.html

9. *September 15, WSB 2 Atlanta* – (Georgia) **Head-on crash shuts down Forsyth County highway.** Highway 20 in Forsyth County, Georgia, reopened September 15 after being closed for more than 2 hours when a head-on collision occurred that involved a Comcast Xfinity vehicle and another vehicle, causing one vehicle to drive

into a ditch. Both drivers sustained non-life-threatening injuries.
Source: http://www.wsbtv.com/news/news/local/police-investigate-head-crash-highway-20-near-hear/nnfx9/

10. *September 15, WITI 6 Milwaukee* – (Wisconsin) **Fatal wreck: one dead after stolen vehicle being pursued by trooper hits semi.** Both northbound and southbound lanes of 1-43 in Belgium, Wisconsin, were shutdown overnight September 15 when a fatal head-on collision occurred after a stolen vehicle traveled across the median and struck a semi-truck causing it to burst into flames. One driver was killed and officials are investigating the incident after finding drug paraphernalia, marijuana, and a loaded handgun inside the stolen car.
Source: http://fox6now.com/2015/09/15/fiery-wreck-ozaukee-co-sheriff-state-patrol-deal-with-wreck-on-i-43/

11. *September 15, WMAQ 5 Chicago* – (Indiana) **Chicago passenger charged with hitting flight attendant, forcing emergency landing.** An American Airlines flight traveling from Miami to Chicago made an emergency landing at Indianapolis International Airport September 14 after an unruly passenger allegedly hit a flight attendant and another passenger during the flight. The passenger was arrested and charged for battery with injury, battery without injury, and disruption of operation of an aircraft, among other charges.
Source: http://www.nbcchicago.com/traffic/transit/Chicago-Passenger-Charged-With-Hitting-Flight-Attendant-Forcing-Emergency-Landing-327709501.html

12. *September 15, Kingston Daily Freeman* – (New York) **Bomb squad removes 'improvised explosive devise' from Saugerties apartment.** New York police reported that surrounding homes were evacuated and all lanes of U.S. Route 9W were shut down September 15 for nearly 3 hours while bomb squads cleared the scene after a contractor found an improvised explosive device at the Carriage House in Saugerties. The device was removed and determined to be incendiary and an investigation remains ongoing.
Source: http://www.dailyfreeman.com/general-news/20150915/bomb-squad-removes-improvised-explosive-device-from-saugerties-apartment

13. *September 14, KNBC 4 Los Angeles* – (California) **NB 710 Freeway in Long Beach reopens following fatal big rig crash.** All northbound lanes of 710 Freeway in Los Angeles reopened September 14 after a semi-truck overturned and blocked lanes for several hours, leaving 1 man dead. Authorities are investigating the cause of the accident.
Source: http://www.nbclosangeles.com/news/local/NB-710-Freeway-in-Long-Beach-Shut-Down-Following-Fatal-Big-Rig-Crash--327462091.html

Food and Agriculture Sector

14. *September 15, Associated Press* – (National) **FDA bans sales of 4 R.J. Reynolds cigarette brands.** The U.S. Food and Drug Administration (FDA) banned sales of four cigarette brands from North Carolina-based R.J. Reynolds due to failure to comply with

FDA safety review regulations including failure to show that its new products do not raise new safety concerns September 15.The brands recalled were Came Crush Bold, Pall Mall Deep Set Recessed Filer, Fall Mall Deep Set Recessed Filter Menthol, and Vantage Tech 13.
Source: https://www.bostonglobe.com/business/2015/09/15/fda-halts-sales-reynolds-cigarette-brands/CKp8hpEwRf2ZcZ054CYz1K/story.html

15. *September 15, Portland Oregonian* – (National) **Numbers surpass 400 in Salmonella outbreak linked to cucumbers.** The Centers of Disease Control and Prevention reported September 15 that a nationwide Salmonella outbreak linked to imported cucumbers continues to spread with more than 400 people sickened in 31 states, and 2 confirmed deaths.
Source:
http://www.oregonlive.com/health/index.ssf/2015/09/numbers_surpass_400_in_salmon e.html

16. *September 15, U.S. Food and Drug Administration* – (National) **Iowa Select Herbs, LLC issues a nationwide recall of its products pursuant to a consent decree issued by the Federal Court of the Northern District of Iowa.** Cedar Rapids-based Iowa Select Herbs, LLC is recalling inventory sold from January – August in compliance with a Consent Decree issued by the Federal court of the Northern District of Iowa in which unapproved new drugs, misbranded drugs, misbranded dietary supplements, and dietary supplements did not meet compliance with current Good Manufacturing Practice regulations for Dietary Supplements, and therefore adulterated. The recalled products were sold nationwide to wholesalers and consumers using the company's Web site and through Internet sales.
Source: http://www.fda.gov/Safety/Recalls/ucm462536.htm

17. *September 14, U.S. Department of Labor* – (Wisconsin) **OSHA cites Country Vision Cooperative for exposing workers to bin hazards.** The Occupation Safety and Health Administration cited the Chilton Facility for 1 willful and 3 serious safety violations after an investigation revealed that the facility failed to turn off power sources to augers before allowing employees to enter grain storage bins, exposing them to amputation hazards as well as the possibility of being engulfed in moving grains, among other findings. Proposed fine total $70,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEA SES&p_id=28707

Water and Wastewater Systems Sector

18. *September 16, CNN* – (Utah) **Floods in Utah kill 16, leave four missing.** Residents in Hildale, Utah, and Colorado City, Arizona, were issued boil water advisory September 14 after a flash flood damaged surrounding areas and carried vehicles and debris throughout the city, killing 16 people and injuring several others.
Source: http://www.cnn.com/2015/09/15/us/utah-arizona-flooding/index.html

19. *September 15, Southern California City News Service; LA Weekly* – (California) **Storm sends raw sewage into L.A. River.** Long Beach officials reported September 15 that about 420,000 gallons of sewage water flowed into the California ocean after storm waters overran a 24-inch sewage pipe that was temporarily exposed while construction crews worked on the pipe. Officials reported Long Beach will be closed for several days.
Source: http://www.laweekly.com/news/storm-sends-raw-sewage-into-la-river-6045211

For another story, see item **7**

Healthcare and Public Health Sector

20. *September 16, Associated Press* – (California) **California surgeon charged in $150M insurance scam.** A Los Angeles-based orthopedic surgeon was charged in an indictment unsealed September 15 for working with 14 associates to bilk insurance companies out of $150 million through unnecessary operations performed by untrained staff. The orthopedic surgeon allegedly conspired to pay attorneys and marketers up to $10,000 a month to illegally refer patients, 21 of which sustained lasting scars and required additional surgeries.
Source: http://www.foxnews.com/us/2015/09/16/california-surgeon-charged-in-150-million-insurance-scam/

21. *September 15, WPLG 10 Miami* – (Florida) **North Broward Hospital District to pay government $69.5 million.** The U.S. Department of Justice announced September 15 that the North Broward Hospital District will pay $69.5 million to settle allegations that it violated the Stark Statute and the False Claims Act by allegedly providing compensation to 9 physicians that exceeded the fair market value of their services.
Source: http://www.local10.com/news/north-broward-hospital-district-to-pay-government-695-million/35281104

22. *September 15, WVUE 8 New Orleans* – (Louisiana; Mississippi) **Confidential patient information exposed after computer theft.** The Louisiana State University Health New Orleans School of Medicine announced September 15 that the personal and medical information of approximately 5,000 patients from Louisiana and Mississippi may have been accessed after a laptop was stolen from a faculty member's car in July.
Source: http://www.fox8live.com/story/30038755/patient-information-exposed-after-computer-theft

Government Facilities Sector

23. *September 16, Philadelphia Daily News* – (Pennsylvania) **N. Philly man indicted for defrauding feds in computer scam.** A man from north Philadelphia was charged September 14 for allegedly defrauding a Federal program that donates Federal agencies' unused computer equipment to schools and educational nonprofits, by claiming to represent a U.S. Internal Revenue Service-recognized tax-exempt organization and filing phony paperwork in 2013 in order to obtain at least 96 computer

monitors.
Source:
http://www.philly.com/philly/news/20150916_N__Philly_man_indicted_for_defrauding_feds_in_computer_scam.html

24. *September 16, Reuters* – (National) **Homeland Security websites vulnerable to cyber attack: Audit.** The Office of the Inspector General for DHS released a report September 15 citing several deficiencies within DHS' information systems including lapses in internal systems used by several agencies that may allow unauthorized individuals to gain access to sensitive data, and the need to establish a cyber-training program for analysts and investigators, among other findings.
Source: http://www.aol.com/article/2015/09/16/homeland-security-websites-vulnerable-to-cyber-attack-audit/21236663/

25. *September 15, Ironton Tribune* – (Ohio) **Ironton High School closed for bomb threat.** Ironton High School in Ohio was closed September 15 after the school received an anonymous email containing a bomb threat. An investigation into the source of the threat is ongoing.
Source: http://www.irontontribune.com/2015/09/15/ironton-high-school-closed-for-bomb-threat/

26. *September 15, KFSN 30 Fresno* – (California) **Rough Fire evacuation orders lifted for Dunlap, Miramonte, and Pinehurst.** Mandatory evacuation orders for residents in Dunlap, Miramonte, and Pinehurst were lifted after crews reached 49 percent containment September 15 of the 139,000-acre Rough Fire burning around Fresno, California.
Source: http://abc30.com/news/rough-fire-evacuation-orders-lifted-for-dunlap-miramonte-and-pinehurst/985739/

27. *September 15, Associated Press* – (Washington) **Striking Seattle teachers to return to classroom.** Seattle Public Schools reported that schools were expected to reopen September 17 for 53,000 students in the city after the district reached a tentative agreement with teachers who have been on strike since September 9.
Source: http://www.msn.com/en-us/news/us/striking-seattle-teachers-to-return-to-classroom/ar-AAekMqo

28. *September 15, KABC 7 Los Angeles* – (California) **Inglewood elementary school evacuated due to foul odor.** Thirteen people were transported to an area hospital following reports of a foul odor at La Tijera K-8 Academy of Excellence Charter School in Inglewood, prompting the evacuation of the building September 15. Authorities are investigating the source of the odor after tests results for a gas leak came out negative.
Source: http://abc7.com/news/inglewood-elementary-school-evacuated-due-to-foul-odor/986206/

Emergency Services Sector

Nothing to report

Information Technology Sector

29. *September 16, Securityweek* – (International) **Major malvertising operation went undetected for three weeks.** Security researchers from Malwarebytes discovered a malvertising campaign affecting Web sites of several major companies including eBay, Drudge Report, and Answers.com, in which attackers were able to redirect victims to malware-serving Web sites containing the Angler exploit kit (EK) by loading ads through a rogue ad server. The campaign went undetected for nearly three weeks, and 46 percent of the affected users were in the U.S.
Source: http://www.securityweek.com/major-malvertising-operation-went-undetected-three-weeks

30. *September 16, Help Net Security* – (International) **Persistent XSS flaw in SharePoint 2013 revealed, patched.** Microsoft patched a persistent cross-site scripting (XSS) vulnerability in SharePoint 2013 in which an attacker could obtain information about a user's operating system (OS), browser, plugins, and other information in order to steal sensitive information, gain control of the system, and download and execute malicious code remotely.
Source: http://www.net-security.org/secworld.php?id=18860

31. *September 16, Securityweek* – (International) **WordPress patches XSS, privilege escalation vulnerabilities.** The developers of WordPress released version 4.3.1 content management system (CMS) addressing 3 vulnerabilities and 26 bugs, including a cross-site scripting (XSS) flaw related to the processing of shortcode tags in which an attacker could inject malicious JavaScript code into objects rendered on WordPress pages, a flaw that allows users to publish private "sticky" posts that can be combined with the XSS vulnerability, and a separate XSS vulnerability.
Source: http://www.securityweek.com/wordpress-patches-xss-privilege-escalation-vulnerabilities

32. *September 16, Help Net Security* – (International) **Android 5 bug allows attackers to easily unlock password-protected devices.** The University of Texas at Austin Information Security Office discovered a lockscreen bypass vulnerability affecting Android version 5.1.1 in which an attacker could use a large string password with the camera app open to crash the password lockscreen and gain full access to the device. Google addressed the issue in Android 5.1.1 build LMY48M.
Source: http://www.net-security.org/secworld.php?id=18858

33. *September 16, Threatpost* – (International) **Bug in iOS allows writing of arbitrary files via AirDrop.** Researchers from Azimuth Security discovered a vulnerability in a library of Apple's iOS and OS X operating systems which an attacker could leverage via AirDrop with or without the user's approval to execute a director traversal attack, and arbitrarily write files to any location in an affected device's file system.

Source: https://threatpost.com/bug-in-ios-and-osx-allows-writing-of-arbitrary-files-via-airdrop/114681/

34. *September 15, The Register* – (International) **Thought Heartbleed was dead? Nope – hundreds of thousands of things still vulnerable to attack.** The founder of the Shodan search engine reported that over 200,000 devices on the Internet are still vulnerable to the Heartbleed OpenSSL vulnerability discovered in 2014, including 57,272 devices in the U.S. The vulnerability allows an attacker to extract passwords and other sensitive information due to a missing bounds check that allowed repeated data checks from server memory.
Source: http://www.theregister.co.uk/2015/09/15/still_200k_iot_heartbleed_vulns/

35. *September 15, Agence France-Presse* – (International) **Russian pleads guilty in major hacking case.** A Russian national arrested in 2012 and extradited to the U.S. in February 2015 pleaded guilty September 15 to leading a hacking and data breach scheme that compromised the Nasdaq stock market and payment systems at 7-Eleven, Carrefour, JC Penny, and other companies, resulting in losses of over $300 million between 2005 and 2012.
Source: http://www.securityweek.com/russian-pleads-guilty-major-hacking-case

For another story, see item **24**

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

36. *September 14, WJXX 25 Jacksonville; WTLV 12 Jacksonville* – (Florida) **Retirement community upset over phone and internet outages.** All 450 AT&T customers residing in The Cascades in St. Augustine, were without phone or Internet service for 5 days following severe weather that damaged landline service. Crews repaired the damage landline September 14.
Source: http://www.firstcoastnews.com/story/news/2015/09/14/--not--inconvenience---dangerous/72279836/

For additional stories, see items **7**, **32**, and **33**

Commercial Facilities Sector

37. *September 15, KTVI 2 St. Louis* – (Missouri) **Brentwood Community Center evacuated for ammonia leak.** A line to an ammonia tank broke at the Brentwood Community Center ice rink while contractors were working, causing an ammonia leak that sent 8 people to area hospitals and closed the facility for 48 hours while the ice

returned to normal September 15. Officials reported that all activities scheduled until September 17 will be postponed.
Source: http://fox2now.com/2015/09/15/building-evacuated-for-ammonia-leak-in-brentwood/

For additional stories, see items **7** and **35**

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.