Daily Open Source Infrastructure Report
15 July 2014

Top Stories

- Citigroup announced July 14 that it would pay $7 billion to settle U.S. Department of Justice charges that the financial institution knowingly sold risky mortgage-based securities prior to the 2008 financial crisis. – *USA Today* (See item **10**)

- One person was killed and 24 others were injured when a Greyhound bus and a vehicle traveling in the wrong direction collided on Interstate 70 near Richmond, Indiana, July 13, closing the highway for several hours. – *WHIO 7 Dayton* (See item **16**)

- Bell County, Texas officials placed residents under emergency water restrictions after a contractor struck a main water transmission line July 12, impacting surrounding areas and the Fort Hood U.S. Army post. – *KCEN 6 Temple* (See item **22**)

- Cyphort researchers reported identifying a cybercriminal operation known as "NightHunter" that has been active since 2009 and uses various pieces of malware and keyloggers to target organizations in the energy, education, health, insurance, and charity industries. – *Securityweek* (See item **31**)

Fast Jump Menu

Energy Sector

1. *July 13, Forum of Fargo-Moorhead* – (North Dakota) **760 barrels of oil reported stolen in North Dakota oil patch.** Authorities are investigating after about 760 barrels of crude oil worth an estimated $80,000 were stolen from tanks at two Cornerstone Natural Resources-owned well sites near Dunn County. K&R Roustabout reported the theft after a worker maintaining the tanks reported that the amount of oil calculated came up short.
   Source: http://www.twincities.com/nation/ci_26137613/760-barrels-oil-reported-stolen-north-dakota-oil

2. *July 12, Associated Press* – (New Mexico) **Air pollution allegations lead to settlement in NM.** Regency Field Services LLC reached a settlement with the New Mexico Environment Department July 11 and agreed to pay nearly $70,000 to settle violations at its natural gas plant in Santa Fe which included failure to demonstrate compliance with certain emissions limits and failure to maintain certain records. The plant was also accused of failing to conduct certain tests and not checking if monitoring equipment was working properly.
   Source: http://www.washingtontimes.com/news/2014/jul/12/air-pollution-allegations-lead-to-settlement-in-nm/

For another story, see item **31**

[Return to top]

Chemical Industry Sector

3. *July 14, WGOW 1150 AM Chattanooga* – (Tennessee) **Workers evacuate after chemical company Haz-Mat fire.** Between 2,000 and 3,000 gallons a caustic soda spilled and started a fire at the JIT Chemicals facility in Chattanooga while workers were transferring a sodium hydroxide solution from a barge into a storage tank July 11. One worker was contaminated and transported to an area hospital, and crews extinguished the blaze and cleaned the spill.
   Source: http://www.wgowam.com/common/more.php?m=58&ts=1405106409&article=4713D13D092E11E4B51EFEFDADE6840A&mode=2

4. *July 13, WGRZ 2 Buffalo* – (New York) **Tonawanda fire crews douse chemical fire.** Employees at a PeroxyChem facility in Tonawanda were evacuated and the sprinkler system inside the warehouse was triggered July 12 when a chemical substance caught fire in oxidizer equipment and started smoking. Firefighters responded and investigators are searching for the cause of the fire.
   Source: http://www.wgrz.com/story/news/local/tonawandas/2014/07/12/tonawanda-fire-crews-douse-chemical-fire/12587297/

5. *July 11, KPRC 2 Houston* – (Texas) **Highway 59 reopens after truck carrying explosive chemicals closes freeway.** The refrigeration system on a FedEx truck

carrying 200 gallons of liquefied peroxide, a chemical that explodes when it is rises above 50 degrees, malfunctioned along Highway 59 in Liberty County July 11, prompting the closure of the freeway and evacuation of a business. The driver pulled the vehicle off the road and HAZMAT crews took protective actions to avoid an explosion and clear the scene, allowing the freeway to reopen.
Source: http://www.click2houston.com/news/truck-carrying-explosive-chemical-shuts-down-hwyy-59-in-liberty-county/26911020

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

6. *July 11, Lacey Patch* – (New Jersey) **Oyster Creek shut down again for second time this week.** The operators of the Oyster Creek Generating Station in New Jersey took the plant's reactor off line July 11 after detecting a reduction in steam condenser vacuum. The shutdown was the second in the past week following a July 7 shutdown due to degradation in five electromatic relief valves.
Source: http://lacey.patch.com/groups/business-news/p/oyster-creek-shut-down-again-for-second-time-this-week

[Return to top]

Critical Manufacturing Sector

7. *July 13, Wausau Daily Herald* – (Wisconsin) **Fire causes $2 million in damage to Merrill factory.** Firefighters responded July 13 to a fire at Northern Wire LLC in Merrill in the metal plating area of the facility. Damages from the fire were estimated at $2 million.
Source: http://www.wausaudailyherald.com/story/news/local/2014/07/13/fire-damages-merrill-factory/12593279/

[Return to top]

Defense Industrial Base Sector

8. *July 14, The Register* – (International) **FBI: We found US MILITARY AIRCRAFT INTEL during raid on alleged Chinese hacker.** A Chinese man was arrested by Canadian authorities at the request of the FBI for working with two other uncharged suspects and allegedly hacking into several defense contractors' networks in the U.S. and Europe in order to steal information on 32 U.S. projects, including the U.S. Lockheed F-22 and F-35 aircraft and Boeing's C-17 cargo plane. Authorities alleged the suspects were able to extract several thousand digital files and attempted to sell the information off to State-owned companies in China.
Source: http://www.theregister.co.uk/2014/07/14/us_military_aircraft_intel_captured_in_alleged_chinese_hacker_raid/

9. *July 13, Reuters* – (International) **'Excessive' rubbing of engine blades caused F-35 failure: Pentagon.** U.S. Department of Defense officials announced July 13 that excessive rubbing of fan blades likely caused a June 23 engine fire on a U.S. Air Force F-35 that resulted in a grounding of the entire fleet. Authorities stated that investigations did not reveal signs of similar wear on any of the remaining 97 aircraft in the fleet and the issue does not appear to be a design flaw.
Source: http://www.reuters.com/article/2014/07/13/us-airshow-britain-f-idUSKBN0FI0XD20140713

[Return to top]

Financial Services Sector

10. *July 14, USA Today* – (National) **Citi to pay $7 billion in Justice settlement.** Citigroup announced July 14 that it would pay $7 billion to settle U.S. Department of Justice charges that the financial institution knowingly sold risky mortgage-based securities prior to the 2008 financial crisis.
Source: http://www.usatoday.com/story/money/business/2014/07/14/justice-citi-7-billion-dollar-settlement/12616741/

11. *July 14, Securityweek* – (International) **Kronos: New financial malware sold on Russian underground forum.** Researchers with Trusteer reported July 11 that a new piece of banking malware known as Kronos has recently been advertised on a Russian underweb forum in a pre-release sale. The malware contains HTML injection and form-grabbing capabilities, allegedly works with modern and older Web browsers, and is compatible with the Zeus trojan.
Source: http://www.securityweek.com/kronos-new-financial-malware-sold-russian-underground-forum

12. *July 13, Baton Rouge Advocate* – (National) **Hedge fund owner pleads guilty to mail fraud.** A Zachary, Louisiana hedge fund manager who operated Greenwing Capital Management LLC pleaded guilty July 11 to defrauding investors in Louisiana, Florida, Mississippi, and Texas of around $13 million by delivering false statements to investors showing profits when most investments failed or were used by the hedge fund owner for personal use.
Source: http://theadvocate.com/home/9696542-125/hedge-fund-owner-pleads-guilty

13. *July 11, Dark Reading* – (International) **International hacker pleads guilty to 2011 global cyberattack.** A member of an international cybercrime organization pleaded guilty July 11 for working with co-conspirators to hack into the payment card processor for the American Red Cross in 2011 and stealing payment card data that was then used to make $14 million in fraudulent ATM withdrawals around the world.
Source: http://www.darkreading.com/international-hacker-pleads-guilty-to-2011-global-cyberattack/d/d-id/1297241

For additional stories, see items **25** and **31**

[Return to top]

Transportation Systems Sector

14. *July 14, Associated Press* – (New Jersey) **PATH trains rolling hours after derailment.** Four people were hurt and 200 passengers were evacuated when a Port Authority of New York and New Jersey train derailed July 13 after it struck a box truck that was crossing the tracks in Harrison. Service resumed July 14 and the incident is under investigation.
Source: http://www.stltoday.com/news/national/path-trains-rolling-hours-after-derailment/article_412c22f5-83e1-5c90-9c7e-8a9c18576774.html

15. *July 13, Associated Press* – (New Jersey) **Air India flight lands safely after engine fire.** An outbound Air India flight with 313 passengers headed for Mumbai from Newark Liberty International Airport returned to the New Jersey airport July 13 when an engine caught fire on the plane's left side shortly after takeoff and shut down. The plane was able to land safely and no injuries were reported.
Source: http://abcnews.go.com/US/wireStory/flight-lands-safely-bird-strike-sparks-fire-24545168

16. *July 13, WHIO 7 Dayton* – (Indiana) **Greyhound bus in fatal crash was to make stop in Dayton.** One person was killed and 24 others were injured when a Greyhound bus and a vehicle traveling in the wrong direction collided on Interstate 70 near Richmond, Indiana, July 13, closing the highway for several hours. Greyhound is working with authorities to investigate the incident.
Source: http://www.whio.com/news/news/crime-law/greyhound-bus-fatal-crash-was-headed-dayton/ngfJg/

17. *July 11, Associated Press* – (Wyoming) **Bus carrying Chinese tourists crashes in Wyoming.** U.S. 89 north of Colter Bay Village on Jackson Lake in Wyoming was closed for about 5 hours July 10 when a bus carrying tourists overcorrected and flipped over on its side, hospitalizing 27 people.
Source: http://www.miamiherald.com/2014/07/11/4230616/dozens-taken-to-hospital-in-teton.html

18. *July 11, Daytona Beach News-Journal* – (Florida) **Police: Palm Coast woman stole $150K from Daytona airport services firm.** A former employee of Yelvington Jet Aviation operating out of Daytona Beach International Airport was charged July 10 after an investigation found that she unlawfully spent more than $156,000 of company credit on personal purchases over 5 years.
Source: http://www.news-journalonline.com/article/20140711/NEWS/140719849/1040

19. *July 11, Associated Press* – (Montana) **BNSF train derails near Worden; 13 cars off track.** Thirteen cars from a Burlington Northern Santa Fe (BNSF) coal train derailed about 35 miles east of Billings July 10, closing the rail line. The cause for the derailment is under investigation and the rail line was scheduled to reopen July 12.
Source: http://www.greatfallstribune.com/story/news/local/2014/07/11/bnsf-train-

derails-near-worden-cars-tracks/12543891/

For another story, see item **5**

Food and Agriculture Sector

20. *July 13, KMGH 7 Denver* – (Colorado) **24 people exposed to fumes at Longmont restaurant.** Authorities believe a 200-gallon water heater malfunctioned and sent chemical fumes throughout the Oskar Blues restaurant in Longmont July 13, prompting the decontamination of at least 24 employees, including 17 individuals that were transported to area hospitals with symptoms including vomiting and respiratory and eye irritation.
Source: http://www.thedenverchannel.com/news/local-news/24-people-exposed-to-chemicals-at-longmont-restaurant

Water and Wastewater Systems Sector

21. *July 14, Mlive.com*– (Michigan) **Water main break repaired but water boil advisory continues for Vicksburg.** A main water break that previously led to a boil water advisory in Vicksburg, Michigan, was repaired but residents remained under a boil water notice July 13.
Source:
http://www.mlive.com/news/kalamazoo/index.ssf/2014/07/water_main_break_repaired_but.html

22. *July 14, KCEN 6 Temple* – (Texas) **Residents asked to conserve water after Bell County water main break.** Bell County officials asked residents served by the Bell County Water Control and Improvement District #1, including residents in the City of Killeen and the Fort Hood U.S. Army post, to limit water usage after a contractor struck a main water transmission line July 12, causing the line to lose 50 gallons of water per minute. Water service continued from reserves and affected areas were placed under emergency water restrictions that also closed restaurants in Copperas Cove.
Source: http://www.kcentv.com/story/26006300/residents-asked-to-conserve-water-after-bell-county-water-main-break

Healthcare and Public Health Sector

See item **31**

Government Facilities Sector

23. *July 13, Associated Press* – (California) **Man accused of starting N. California wildfire.** Officials arrested a suspect July 12 accused of causing a fire after the exhaust from his truck ignited the 3,700-acre Bully Fire in Redding as he was delivering material to a marijuana cultivation site in Shasta County. Crews reached 10 percent containment July 13 of the wildfire while 15 homes and about 50 other structures remained under threat.
Source: http://news.msn.com/crime-justice/man-accused-of-starting-n-california-wildfire

24. *July 13, KERO 23 Bakersfield* – (California) **Nicolls Fire now more than 1,000 acres, 55 percent contained.** Crews reached 55 percent containment July 13 of the Nicolls Fire after burning 1,447 acres in Bakersfield east of Lake Isabella. Several areas around the fire were closed to the public in the Scodie Mountains, the Sequoia National Forest reported.
Source: http://www.turnto23.com/news/local-news/onyx-fire-burns-above-lake-isabella-071214

25. *July 11, San Francisco Bay City News* – (California) **Former CalPERS CEO pleads guilty to conspiring to accept bribes.** A former California Public Employees Retirement System chief executive officer pleaded guilty July 11 to conspiring to accept bribes to influence the fund's investments and admitted to accepting $250,000 from an investment placement agent in exchange for confidential information about the company's investments. The investment placement agent was also charged for his role in the scheme which included falsifying facts about investor disclosure letters and conspiring to commit fraud.
Source: http://sfappeal.com/2014/07/former-calpers-ceo-pleads-guilty-to-conspiring-to-accept-bribes/

For additional stories, see items **22** and **31**

[Return to top]

Emergency Services Sector

26. *July 13, Miami Herald* – (Florida) **Parts stolen from three Miami Police boats.** Approximately $18,000 worth of lower unit parts were stolen from three Miami Police Department boats over the weekend of July 12, forcing the boats out of service indefinitely. Authorities are investigating the theft which took place at the Miami Yacht Club.
Source: http://www.miamiherald.com/2014/07/13/4234417/parts-stolen-from-three-miami.html

27. *July 12, Associated Press* – (Florida) **Prison guard guilty of stealing inmates' IDs.** A former Zephyrhills Correctional Facility prison guard pleaded guilty July 9 to charges

associated with stealing personal information from Florida Department of Corrections databases and using it to file 182 fake income tax returns seeking more than $500,000.
Source: http://www.naplesnews.com/news/state/prison-guard-guilty-of-stealing-inmates-ids_19623000

28. *July 11, KTVU 2 Oakland* – (California) **Oakland Police: HVAC system was source of odor at headquarters.** Police officers were evacuated and the Oakland Police headquarters in California was closed July 11 when an employee smelled what they believed to be gas prompting an evacuation while crews isolated the odor to the heating and air conditioning system. Officers were allowed back into the building after several hours to retrieve their belongings while the building remained closed to the public until further notice.
Source: http://www.ktvu.com/news/news/crime-law/oakland-police-headquarters-evacuated-due-gas-leak/ngdXx/

Information Technology Sector

29. *July 14, Help Net Security* – (International) **Critical vulnerabilities in web-based password managers found.** Researchers at the University of California identified and reported various vulnerabilities in five Web-based password managers that could allow attackers to obtain a user's credentials. LastPass, My1Login, RoboForm, and PasswordBox reported that they closed the vulnerabilities after they were reported, while the researchers did not receive word on the issues from NeedMyPassword.
Source: http://www.net-security.org/secworld.php?id=17111

30. *July 14, Softpedia* – (International) **Cisco patches four-year-old Apache Struts 2 issue.** Cisco patched a vulnerability in Apache Struts 2 that was reported in 2010 which could allow an attacker to use a malicious Object-Graph Navigation Language (OGNL) expression to compromise vulnerable systems.
Source: http://news.softpedia.com/news/Cisco-Patches-Four-Year-Old-Apache-Struts-2-Issue-450663.shtml

31. *July 11, Securityweek* – (International) **Attackers use keyloggers, email to steal data in "NightHunter" attacks.** Cyphort researchers reported identifying a cybercriminal operation known as "NightHunter" that has been active since 2009 and uses various pieces of malware and keyloggers to target organizations in the energy, education, health, insurance, and charity industries. The campaign distributes the malware through phishing emails that are usually sent to finance, human resources, and sales departments.
Source: http://www.securityweek.com/attackers-use-keyloggers-email-steal-data-nighthunter-attacks

For another story, see item **11**

[Return to top]

Communications Sector

32. *July 14, Palm Springs Desert Sun* – (California) **Time Warner Cable services restored Sunday afternoon.** Internet, phone, and television services were restored to Time Warner Cable customers across several cities in the Coachella Valley area of California July 13 after an outage caused by vandalism to the operator's network July 12.
Source: http://www.desertsun.com/story/news/local/2014/07/13/time-warner-cable-outage/12607277/

[Return to top]

Commercial Facilities Sector

33. *July 14, Help Net Security* – (International) **Keyloggers found at hotel business centers, US Secret Service warns.** U.S. officials issued an advisory to hospitality industry companies encouraging them to secure their public computers and limit guest accounts to non-administrator accounts following the arrest of a group of individuals that are suspected of compromising computers in Texas hotel business centers. The suspects allegedly used stolen credit cards to register as hotel guests and used the hotel's business center to download and execute key logging software, which was used to capture the information of other guests.
Source: http://www.net-security.org/secworld.php?id=17110

34. *July 13, CNN* – (New York) **Fire at New York's Rockefeller Center observation deck injures 6.** A camera on an elevated portion of the observation deck at Rockefeller Center in New York City caught fire July 13and sent embers falling onto six visitors standing below, causing minor burns. The fire was extinguished before firefighters arrived and one child was transported to an area hospital for treatment.
Source: http://www.cnn.com/2014/07/13/us/new-york-rockefeller-center-fire/index.html

35. *July 13, CNN* – (Florida) **Dozens evacuated on Disney World monorail after power outage at Epcot Center.** Authorities used a lift to evacuate about 120 people from the monorail train at Walt Disney World's Epcot Center in Florida July 13 after a weather-related power outage at the amusement park caused the train to halt and cut service to the air conditioner onboard.
Source: http://ktla.com/2014/07/13/dozens-evacuated-on-disney-world-monorail-after-

power-outage-at-epcot-center/

36. *July 13, Associated Press; Stamford Advocate* – (Connecticut) **Captured on video, gunman sprays gunfire into crowd outside Stamford nightclub; suspect held.** A Connecticut man was arrested and charged after he fired a weapon dozens of times into a crowd outside a Stamford nightclub July 13, injuring five people.
Source: http://www.foxnews.com/us/2014/07/13/captured-on-video-gunman-sprays-gunfire-into-crowd-outside-stamford-nightclub/

37. *July 13, Associated Press; KOMO 4 Seattle* – (Washington) **5 people shot outside bar in south Seattle suburbs.** One person sustained life-threatening injuries and four others were transported to area hospitals following a July 13 shooting in the parking lot outside a bar in Skyway, Washington. Police are searching for suspects after they determined at least two guns were used in the incident.
Source: http://news.msn.com/crime-justice/5-people-shot-outside-bar-in-south-seattle-suburbs

38. *July 11, WKMG 6 Orlando* – (Florida) **Gastrointestinal illness outbreak investigated at Orlando hotel.** Orange County health officials are investigating a gastrointestinal illness outbreak that sickened several dozen people during their stay at the Orlando World Center Marriott in Florida between June 29 and July 7 while attending a conference.
Source: http://www.clickorlando.com/news/gastrointestinal-illness-outbreak-investigated-at-orlando-hotel/26894720

For additional stories, see items **5** and **22**

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.