Homeland Security

Daily Open Source Infrastructure Report
30 January 2013

Top Stories

- An oil spill caused by a barge colliding with a bridge January 27 forced the closure of a 16-mile stretch of the river causing at least 47 barges and other vessel to idle as crews worked to clean up the oil spill January 29. – *Associated Press* (See item **8**)

- Burglars stole roughly $40,000 worth of copper and tools from a Chesapeake High School athletic center. – *WSAZ 3 Huntington* (See item **17**)

- Very few U.S. online retailers, internet service providers (ISP), and financial institutions have implemented a major vulnerability in the Domain Name System (DNS), five years after the vulnerability was discovered. – *Network World* (See item **20**)

- A security flaw in the firmware of digital video recorders (DVR) made by 19 manufacturers can allow attackers to remotely view, delete, or copy video streams from security cameras networked to the DVRs. – *The Register* (See item **22**)

Fast Jump Menu

PRODUCTION INDUSTRIES	SERVICE INDUSTRIES
• Energy	• Banking and Finance
• Chemical	• Transportation
• Nuclear Reactors, Materials, and Waste	• Postal and Shipping
• Critical Manufacturing	• Information Technology
• Defense Industrial Base	• Communications
• Dams	• Commercial Facilities
SUSTENANCE and HEALTH	**FEDERAL and STATE**
• Agriculture and Food	• Government Facilities
• Water	• Emergency Services
• Public Health and Healthcare	• National Monuments and Icons

---

Energy Sector

1. *January 29, Contra Costa Times* – (California) **Chevron pays $10 million, announces inspection and training reforms after Aug. 6 fire.** After an August 6, 2012 fire, Chevron Corp. paid out $10 million to several entities that were affected, and have taken steps to correct safety failures that led to the fire.
Source: http://www.mercurynews.com/top-stories/ci_22468555/chevron-pays-10-million-announces-inspection-and-training

2. *January 29, Uintah Basin Standard* – (Utah) **Rig fire forces evacuations.** Nearby residents were evacuated near Roosevelt after a blaze following an oil and gas leak January 22.
Source: http://www.ubstandard.com/stories/Rig-fire-forces-evacuations,11529

3. *January 29, Tyler Morning Telegraph; KYTX 19 Nacogdoches* – (Texas) **2 suffer second-degree burns in oil storage tank explosion.** Two victims were taken to a hospital for severe burns after a cigarette-caused explosion at an oil tank storage building in Van Zandt County. Two tanks were on fire and officials were attempting to stop the fire from spreading to the remaining three tanks.
Source: http://www.tylerpaper.com/article/20130129/NEWS01/130129758/-1/NEWS

4. *January 28, U.S. Environmental Protection Agency* – (California) **EPA resolves air violations with Thermal Energy Development Partnership in Tracy, California for $145,000.** Thermal Energy Development Partnership settled a Clean Air Act violation for $145,000 with the U.S. Environmental Protection Agency on claims that the biomass electric power plant did not accurately operate and upkeep emissions monitoring equipment.
Source: http://yosemite.epa.gov/opa/admpress.nsf/0/4FD6A59AAB0C1FF285257B0100682988

   For another story, see item **8**

[Return to top]

Chemical Industry Sector

5. *January 29, Jersey Journal (New Jersey)* – **Plant workers suffer severe chemical burns in Branchburg.** Three employees from AZ Electronic Materials were taken to a hospital January 28 with severe burns and possible ingestion of a chemical after roughly one-gallon was spilled at the facility.
Source: http://www.nj.com/somerset/index.ssf/2013/01/chemical_burns_workers_eyes_fa.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

6. *January 29, Nuclear Street* – (Nebraska) **NRC begins new round of safety inspections at Fort Calhoun, investigates pump installation.** Nuclear Regulatory Commission inspectors began a new on-site inspection of the offline Fort Calhoun nuclear power plant to verify if water pumps are properly bolted down.
Source: http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2013/01/29/nrc-begins-new-round-of-safety-inspections-at-fort-calhoun_2c00_-investigates-pump-installation-012901.aspx

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

7. *January 29, Chicago Sun-Times* – (Illinois) **'People's Attorney' radio show host indicted in $10 million mortgage fraud.** A radio show host was indicted for allegedly participating in a $10 million mortgage scam involving property in the Chicago area.
Source: http://www.suntimes.com/news/metro/17857871-418/peoples-attorney-radio-show-host-indicted-in-10-million-mortgage-fraud.html3

For another story, see item **20**

[Return to top]

Transportation Sector

8. *January 29, Associated Press* – (Mississippi) **Ships idle for Miss. River oil cleanup after crash.** An oil spill caused by a barge colliding with a bridge January 27 forced the closure of a 16-mile stretch of the river causing at least 47 barges and other vessel to idle as crews worked to clean up the oil spill January 29.
Source: http://www.chron.com/news/science/article/Ships-idle-for-Miss-River-oil-cleanup-after-crash-4232193.php

9. *January 28, WXOW19 La Crosse* – (Wisconsin) **Train carrying frac sand derails in Chetek.** A train carrying frac sand derailed in Chetek. A total of 10 cars derailed. The cause of the incident is under investigation.
Source: http://www.wxow.com/story/20756582/2013/01/28/train-carrying-frac-sand-derails-in-chetek

10. *January 28, KTVU 2 Oakland* – (California) **One dead, three injured in Watsonville train-car collision.** Three people were injured and one person died after a cargo train crashed into a car in Watsonville.
Source: http://www.ktvu.com/news/news/local/one-dead-three-injured-watsonville-train-car-colli/nT8cy/

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

Nothing to report

[Return to top]

Water Sector

For another story, see item **8**

[Return to top]

Public Health and Healthcare Sector

11. *January 28, Santa Cruz Sentinel* – (California) **Santa Cruz police nab fake doctor accused of burglarizing area hospitals.** A woman was arrested after stealing credit cards from staff at several hospitals around the Oakland region by impersonating a doctor in order to enter into secured spaces.
Source: http://www.santacruzsentinel.com/localnews/ci_22467936/police-nab-fake-doctor-accused-burglarizing-hospitals-santa?source=most_viewed

12. *January 28, Associated Press – (Minnesota)* **Minn. forum set up to help ease vaccine shortages.** Minnesota's Department of Health is setting up an information sharing forum for health care entities in efforts to curb the shortage of flu vaccines.
Source: http://www.news8000.com/health/Minn-forum-set-up-to-help-ease-vaccine-shortages/-/338/18307404/-/4m8temz/-/index.html

Government Facilities Sector

13. *January 29, Associated Press* – (Rhode Island) **Broken pipe floods Central Falls City Hall.** City officials hope to reopen the Central Falls City Hall within a week after a water pipe burst, likely due to cold weather, and flooded the first and second floors of the building, damaging property and records.
Source: http://www.newstimes.com/news/article/Broken-pipe-floods-Central-Falls-City-Hall-4231684.php

14. *January 29, United Press International* – (International) **U.S. Embassy closes amid Egyptian violence.** Due to recent security concerns in the area, the U.S. Embassy in Cairo, Egypt, ceased all public services January 29.
Source: http://www.upi.com/Top_News/World-News/2013/01/29/US-Embassy-closes-amid-Egyptian-violence/UPI-37741359444600/

15. *January 28, Mississippi Business Journal* – (Mississippi) **Offices move to temporary site in wake of courthouse fire.** The government offices in Webster County were destroyed by a fire January 28 and forced various government agencies to temporarily relocate to the Webster County courthouse.
Source: http://msbusiness.com/blog/2013/01/28/offices-move-to-temporary-site-in-wake-of-courthouse-fire/

16. *January 28, Carlsbad Current-Argus* – (New Mexico) **Bomb threat prompts evacuation of Eddy County Courthouse.** The Eddy County courthouse was evacuated for over 2 hours January 28 while law enforcement checked each floor due to a bomb threat.
Source: http://www.currentargus.com/ci_22466477/bomb-threat-prompts-evacuation-eddy-county-courthouse

17. *January 28, WSAZ 3 Huntington* – (Ohio) **Copper thieves target high school athletic complex.** Burglars stole roughly $40,000 worth of copper and tools from a Chesapeake High School athletic center.
Source: http://www.wsaz.com/news/headlines/Copper-Thieves-Target-High-School-Athletic-Complex--188753681.html

Emergency Services Sector

18. *January 28, WAFF 48 Huntsville* – (Alabama) **Police: Drunk patient flees in stolen ambulance.** A Boaz man was charged after he stole an ambulance that transported him to the emergency room after a car accident.
Source: http://www.wsfa.com/story/20744881/police-drunk-man-flees-hospital-in-stolen-ambulance

19. *January 28, WFAA 8 Dallas* – (Texas) **Man arrested for aiming laser pointer at Dallas police chopper.** A Dallas Police Department surveillance pilot's vision was impaired when a man aimed a laser pointer at the aircraft January 28. Police were able to pinpoint the man's location and arrest him.
Source: http://www.khou.com/news/texas-news?fId=188653811&fPath=/news/local/&fDomain=10247

[Return to top]

Information Technology Sector

20. *January 29, Network World* – (International) **5 years after major DNS flaw is discovered, few US companies have deployed long-term fix.** Very few U.S. online retailers, internet service providers (ISP), and financial institutions have implemented a major vulnerability in the Domain Name System (DNS), five years after the vulnerability was discovered.
Source: http://www.networkworld.com/news/2013/012913-dnssec-266197.html

21. *January 29, Softpedia* – (International) **Over 16,000 Facebook account credentials stolen by PokerAgent botnet.** Researchers at ESET analyzed a botnet known as PokerAgent that stole the login and payment information of over 16,000 Facebook users in 2012. The malware used targeted players of Zynga Poker, infecting at least 800 computers.
Source: http://news.softpedia.com/news/Over-16-000-Facebook-Account-Credentials-Stolen-by-PokerAgent-Botnet-324997.shtml

22. *January 29, The Register* – (International) **Hackers squeeze through DVR hole, break into CCTV cameras.** A security flaw in the firmware of digital video recorders (DVR) made by 19 manufacturers can allow attackers to remotely view, delete, or copy video streams from security cameras networked to the DVRs.
Source: http://www.theregister.co.uk/2013/01/29/cctv_vuln/

23. *January 29, The H* – (International) **iOS update fixes browser vulnerabilities.** Apple released an update for iOS that closes a large number of security vulnerabilities, including some which allowed remote code injection and execution.
Source: http://www.h-online.com/security/news/item/iOS-update-fixes-browser-vulnerabilities-1793259.html

24. *January 29, Softpedia* – (International) **Ruby on Rails 3.0.20 and 2.3.16 released to address extremely critical vulnerability.** The developers of Ruby on Rails released versions 3.0.20 and 2.3.16 and advised users to immediately apply the update to close a major vulnerability in past versions.
Source: http://news.softpedia.com/news/Ruby-on-Rails-3-0-20-and-2-3-16-Released-to-Address-Extremely-Critical-Vulnerability-324866.shtml

25. *January 29, Softpedia* – (International) **Over 85,000 HP printers found to be publicly accessible via the Internet.** A software researcher discovered that over 85,000 printers

made by HP are available via a focused Google search, allowing remote access.
Source: http://news.softpedia.com/news/Over-85-000-HP-Printers-Found-to-Be-Publicly-Accessible-Via-the-Internet-324836.shtml

26. *January 28, CNET* – (International) **Facebook endures hours-long outage in the United States.** A Domain Name System (DNS) issue caused Facebook users to be unable to reach the site for a few hours January 28 if they attempted to reach the site by typing in the URL.
Source: http://news.cnet.com/8301-1023_3-57566336-93/facebook-endures-hours-long-outage-in-the-u.s/

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: https://www.it-isac.org

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

Nothing to report

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

Nothing to report

[Return to top]

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)387-2341
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.