Daily Open Source Infrastructure Report
08 January 2016

Top Stories

- Federal authorities released nutritional recommendations January 7 which include limiting daily added sugar intake and saturated fats to no more than 10 percent daily and limiting sodium intake to less than 2,300 mg a day. – *Los Angeles Times* (See item **9**)
- A suspect was taken into custody following a standoff with police that prompted the 10-hour evacuation of the Tucson, Arizona police substation and crime lab January 6. – *Arizona Daily Star* (See item **17**)
- IOActive reported several vulnerabilities in Drupal's content management system (CMS) including unauthenticated updates that are downloaded unencrypted and a cross-site request forgery (CSRF) vulnerability. – *SecurityWeek* (See item **18**)
- Time Warner Cable reported January 6 that approximately 320,000 of its customers may have had their email passwords stolen through phishing attacks or through data breaches of other companies that stored customer information. – *WGRZ 2 Buffalo* (See item **26**)

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. *January 6, Associated Press* – (North Dakota) **State officials monitor cleanup of pipeline leak that spilled saltwater, oil in Stark County.** The North Dakota Department of Health reported January 6 that an estimated 5,880 gallons of saltwater and 420 gallons of oil leaked from a pipeline at a C12 Energy North Dakota LLC-operated site near Dickinson January 4. Crews reported to the scene and officials are monitoring cleanup efforts.
   Source: http://www.therepublic.com/view/story/bb3e43c4363946ada4d1232a2f2db76c/ND--Saltwater-Spill

2. *January 6, Associated Press* – (California) **California governor declares gas leak a state of emergency.** The governor of California declared a state of emergency January 6 due to a natural-gas leak that has been releasing up to 1,200 tons of methane daily, along with other gases from a Southern California Gas Co.-owned well in Los Angeles. The utility company continues to pay for the relocation of thousands of households while students from two area schools were temporarily moved to other locations.
   Source: http://lasvegassun.com/news/2016/jan/06/california-governor-declares-gas-leak-a-state-of-e/

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

3. *January 6, New London Day* – (Connecticut) **NRC finds 3 violations from October's 'unusual event' at Millstone.** The U.S. Nuclear Regulatory Commission (NRC) cited Dominion-owned Millstone Nuclear Power Station January 5 for three very low safety significance violations for its Unit 2 reactor following an October 4 incident in which a relief valve on the plant's cooling system malfunctioned and leaked 16,570 gallons of reactor coolant. Millstone will be required to enter a corrective action program with the NRC to mitigate future incidences.
   Source: http://www.theday.com/article/20160106/NWS01/160109567

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

See item **23**

Transportation Systems Sector

4. *January 7, Bloomberg News* – (New York) **Uber reaches accord with New York over tracking rider data.** Uber Technologies Inc., and the New York attorney general reached a settlement agreement January 6 following allegations that the company executives had access to rider's location data via a geo-location system called "God View." Uber pledged to encrypt rider location data and require special authentication to access customer information, as well as pay a $20,000 penalty over a September 2014 data breach.
   Source: http://www.buffalonews.com/city-region/state/uber-reaches-accord-with-new-york-over-tracking-rider-data-20160107

5. *January 6, KFMB 8 San Diego* – (California) **Heavy rains cause roof collapse at FedEx facility.** Officials reported January 6 that a San Diego FedEx facility is expected to be closed for several weeks following heavy rains that overwhelmed the drainage system on the roof and cause a 4,000 square foot section of the roof to cave in.
   Source: http://www.cbs8.com/story/30904361/heavy-rains-cause-roof-collapse-at-fedex-facility

6. *January 6, San Luis Obispo Tribune* – (California) **Bomb threat halts SLO Transit bus service; Cal Poly student detained.** San Luis Obispo police and San Luis Obispo (SLO) Transit staff halted all bus service January 6 and detained a California Polytechnic State University student after the student made statements about a potential bomb on a SLO Transit bus. SLO Transit worked to search all 15 buses and normal bus service was expected to resume January 7.
   Source: http://www.sanluisobispo.com/news/local/crime/article53309635.html

7. *January 6, Florida Times-Union* – (Florida) **Fatal accident on northbound U.S. 17 in East Palatka.** Northbound lanes of U.S. 17 reopened January 6 after the highway was shut down for several hours while officials investigated the scene of a fatal crash.
   Source: http://jacksonville.com/news/crime/2016-01-06/story/fatal-accident-northbound-us-17-east-palatka

8. *January 6, WITN 7 Washington* – (North Carolina) **Troopers identify victims in deadly five vehicle crash in Craven County.** Both lanes of U.S. 17 in Ernul were shut down for approximately 5 hours January 6 while crews worked to clear the wreckage from a fatal multi-vehicle crash involving two semi-trucks and three cars that left one driver dead and sent two others to area hospitals.
   Source: http://www.witn.com/home/headlines/Serious-wreck-closes-Craven-County-highway-364395651.html?ref=65

For another story, see item **1**

Food and Agriculture Sector

9. *January 7, Los Angeles Times* – (National) **Eggs and coffee get the all-clear in new**

dietary guidelines just issued by the U.S. The U.S. Department of Agriculture and U.S. Department of Health and Human Services released its nutritional recommendations January 7 dubbed 2015 – 2020 Dietary Guidelines which include limiting daily added sugar intake and saturated fats to no more than 10 percent of daily consumed calories and limiting sodium intake to less than 2,300 mg a day, among other recommendations.
Source: http://www.latimes.com/science/sciencenow/la-sci-sn-dietary-guidelines-eggs-coffee-20160107-story.html

10. *January 7, U.S. Food and Drug Administration* – (National) **Cape Cod Provisions LLC issues allergy alert on undeclared almonds in product.** Massachusetts-based Cape Cod Provisions LLC issued a nationwide recall January 6 for its Cape Cod Cranberry Candy and Harvest Sweets Milk Chocolate/Dark Chocolate/Yogurt Covered Cranberry Blend products due to mislabeling and undeclared almonds. The products were sold in retail locations and mail orders.
Source: http://www.fda.gov/Safety/Recalls/ucm480559.htm

11. *January 7, U.S. Department of Agriculture* – (National) **Neto's Sausage Co., Inc. recalls meat and poultry products produced without benefit of inspection.** The Food Safety and Inspection Service announced January 6 that California-based Neto's Sausage Co., Inc., issued a nationwide recall for 7,687 pounds of its beef, pork, and chicken products in 23 variations that were produced and labeled without the benefit of Federal inspection in house, via online sales, and to a local distributor.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-004-2016-release

12. *January 6, U.S. Food and Drug Administration* – (National) **U.S. Marshals seize dietary supplements containing kratom.** The U.S. Marshals Service at the request of the U.S. Food and Drug Administration seized nearly 90,000 bottles of RelaKzpro dietary supplements in January manufactured by Illinois-based Dordoniz Natural Products LLC due to the products containing kratom, which is categorized as a botanical substance that could pose a risk to public health.
Source:
http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm480344.htm

Water and Wastewater Systems Sector

13. *January 6, St. Louis Post-Dispatch* – (Missouri) **Boil order lifted in High Ridge.** Officials lifted a boil water advisory in the Water District No. 2 service area in High Ridge January 6 once operations were restored at the district's water treatment plant after being shut down due to flooding December 30.
Source: http://www.stltoday.com/news/local/metro/boil-order-lifted-in-high-ridge/article_914c40cc-3ecc-505f-84ce-2ae93ad4f39a.html

Healthcare and Public Health Sector

14. *January 6, Associated Press* – (Indiana) **USB drive with patient info missing from**

Lafayette hospital. Indiana University Health Arnett in Lafayette announced January 6 that an unencrypted USB flash drive containing personal and Protected Health Information (PHI) for 29,324 patients disappeared November 20 from the emergency department. Hospital officials continue to investigate the incident and do not believe any information was used or improperly accessed.
Source: http://www.kansascity.com/news/business/technology/article53316890.html

Government Facilities Sector

15. *January 6, ArmyTimes.com* – (National) **7 more soldiers charged in National Guard recruiting fraud, conspiracy.** The U.S. attorney for the Southern District of New York announced January 6 that seven New York Army National Guard soldiers were arrested and charged for allegedly scheming to obtain fraudulent recruiting bonuses as part of the now-defunct Guard Recruiting Assistance Program (G-RAP) by using online recruiter assistant accounts to falsely claim responsibility in referring soldiers to the New York Guard. The alleged scam dates back to 2007 and the G-RAP was suspended in 2012.
Source: http://www.armytimes.com/story/military/crime/2016/01/06/7-more-soldiers-charged-national-guard-recruiting-fraud-conspiracy/78371086/

16. *January 6, WDSU 6 New Orleans* – (Louisiana) **Gas leak cancels classes Wednesday at Eleanor McMain Secondary School.** Classes at Eleanor McMain Secondary School in New Orleans were cancelled January 6 following a January 5 gas leak due to a burst pipe at a construction site at the school, which prompted an evacuation and dismissal of classes.
Source: http://www.wdsu.com/news/local-news/new-orleans/gas-leak-cancels-classes-wednesday-at-eleanor-mcmain-secondary-school/37295736

For additional stories, see items **2** and **6**

Emergency Services Sector

17. *January 6, Arizona Daily Star* – (Arizona) **Standoff at Tucson police substation ends.** The Tucson police substation and crime lab, along with a trailer park and surrounding businesses were evacuated for approximately 10 hours January 6 after a man parked outside the substation made threats to 9-1-1 dispatchers and threatened to set off propane tanks during a standoff with police. The man was taken into custody without incident.
Source: http://tucson.com/news/blogs/police-beat/standoff-at-tucson-police-substation-ends/article_45cd9798-b48f-11e5-9328-7b5562a3a5cb.html

For another story, see item **25**

Information Technology Sector

18. *January 7, SecurityWeek* – (International) **Unpatched Drupal flaws expose sites to attacks.** A researcher from IOActive reported that there were several vulnerabilities in

the update process for the Drupal content management system (CMS) versions 6 and 7 series including a cross-site request forgery (CSRF) vulnerability that can be exploited to force Web site administrators to check for updates, which can enable hackers to deliver server-side request forgery (SSRF) attacks against drupal.org. Additional issues included an authentication vulnerability that allows hackers to launch Man-in-the-Middle (MitM) attacks due to Drupal's lack of authentication checks, allowing hackers to deliver backdoored versions of Drupal modules to compromise a Web site, among other vulnerabilities.
Source: http://www.securityweek.com/unpatched-drupal-flaws-expose-sites-attacks

19. *January 7, SecurityWeek* – (International) **WordPress 4.4.1 patches XSS vulnerability.** WordPress released security and maintenance updates within version 4.4.1 for its content management system (CMS) that resolved 1 vulnerability and 52 non-security issues including a cross-site scripting (XSS) vulnerability that allowed hackers to compromise infected Web sites.
Source: http://www.securityweek.com/wordpress-441-patches-xss-vulnerability

20. *January 7, Help Net Security* – (International) **HTTPS Bicycle attack reveals password length, allows easier brute-forcing.** A security researcher released a report detailing how a new attack, named HTTPS Bicycle attack can enable hackers to discover the length of a users' password to web applications and potentially make a Web site or browser more susceptible to brute-force attacks by analyzing and using a packet capture of a user's Hypertext Transfer Protocol Secure (HTTPS) traffic and the plaintext HTTP headers included in each and every request. The researcher offered preventative measures such as including hashing or padding the passwords to disguise its length.
Source: http://www.net-security.org/secworld.php?id=19295

21. *January 7, The Register* – (International) **Mozilla warns Firefox fans its SHA-1 ban could bork their security.** Mozilla advised its users to update its Firefox web browser to the latest iteration as users may not have access to Web sites with Secure Hash Algorithm 1 (SHA-1) signed Secure Sockets Layer (SSL) certificate due to the company's rejection of SHA-1-signed certificates, which could allow attackers to spy on users' activities without the users' consent. The company reported that Web sites with the SHA-1-signed certificate were blocked and could not be accessed.
Source:
http://www.theregister.co.uk/2016/01/07/mozilla_warns_firefox_users_that_sha1_ban_could_bork_their_security/

22. *January 6, SecurityWeek* – (International) **Backdoors not patched in many Juniper firewalls.** A security researcher reported that Juniper Networks NetScreen devices were still vulnerable to firewall backdoors after an Internet-wide scan revealed that a total of 1,595 devices had potentially unpatched firewalls. The backdoors can be accessed with any username and the "<<<%s(un='%s') = %u" password.
Source: http://www.securityweek.com/backdoors-not-patched-many-juniper-firewalls

23. *January 6, Softpedia* – (International) **Facebook disabled page scam wants your credit card data, Facebook and PayPal credentials.** Researchers from RNLI and Malwarebytes reported that a new scam has been targeting Facebook Pages users into disclosing their Facebook login credentials, their PayPal credentials, and credit card details by spreading the scam via comments left on Facebook pages that demand owners to access a link or have their pages disabled.
Source: http://news.softpedia.com/news/facebook-disabled-page-scam-wants-your-credit-card-data-facebook-and-paypal-credentials-498557.shtml

24. *January 6, Softpedia* – (International) **Windows and Linux malware linked to Chinese DDoS tool.** Researchers from Malware Must Die! reported that the malware, dubbed Linux/DDOSTF primarily targets Linux systems running Elasticsearch servers, with some attacks against Microsoft Windows systems, via a PHP-MySQ webshell that exploits the Windows Management Instrumentation (WMI) infrastructure, enabling attackers to infiltrate the system, upload and execute malicious exploits, and gain system privileges over the infected machine. The malware is distributed as a malicious executable and linkable format (ELF) and shares similarities to an older malware named JrLinux.
Source: http://news.softpedia.com/news/windows-and-linux-malware-linked-to-chinese-ddos-tool-498554.shtml

For additional stories, see items **4** and **26**

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

25. *January 6, KERO 23 Bakersfield* – (California) **AT&T customers experiencing phone outage in Kern Valley.** AT&T reported that cellular phone service, including 9-1-1 calls, was down in the Kern Valley area January 6. Service was expected to be restored by January 7.
Source: http://www.turnto23.com/news/local-news/att-customers-experiencing-phone-outages-in-ridgecrest

26. *January 6, WGRZ 2 Buffalo* – (National) **Email and password breach at Time Warner.** Time Warner Cable reported January 6 that approximately 320,000 of its customers may have had their email passwords stolen after login credentials were reportedly gathered through malware via phishing attacks or through data breaches of other companies that stored customer information.
Source: http://www.wgrz.com/story/news/2016/01/06/email-and-password-breach-time-warner/78395074/

Commercial Facilities Sector

27. *January 6, Riverside Press-Enterprise* – (California) **Riverside: Business owner accused in manufacturing embezzlement case.** Federal authorities announced January 6 that the owner of FI Products was arrested January 5 in connection to an embezzlement scheme where the owner and three co-conspirators allegedly stole $8 million over a 6-year period from Gardena-based CM Laundry and two other businesses for services provided to Citizens of Humanity.
Source: http://www.pe.com/articles/accused-791037-anguiano-release.html

28. *January 6, Press of Atlantic City* – (New Jersey) **Impaired mom with children car crashed into EHT motel, cops say.** A woman was charged January 6 with multiple motor vehicle violations, child endangerment, and possession of drug paraphernalia after she lost control of her vehicle and struck the corner of the Rex Motel in Egg Harbor Township, leaving the building structurally unsound.
Source: http://www.pressofatlanticcity.com/communities/eht/impaired-mom-with-child-in-car-crashed-into-eht-motel/article_dce24ed8-b4c8-11e5-9c06-cf48aa69d604.html

29. *January 4, Winston-Salem Journal* – (North Carolina) **Bomb scare prompts evacuation at church.** Approximately 150 children were evacuated from a day-care center at First Baptist Church in Winston-Salem January 4 after police received a report of a suspicious package at the church. Police investigated the package before declaring it safe after about 2 hours.
Source: http://m.journalnow.com/news/local/police-determine-suspicious-package-at-church-in-downtown-winston-salem/article_22ba3ccd-290c-55f5-909c-d5c291ca8bc7.html?mode=jqm

For another story, see item **23**

Dams Sector

30. *January 6, Aiken Standard* – (South Carolina) **Aiken County officials to receive $1.5M federal grant for Langley Dam repairs.** The Aiken County Council announced January 5 that the county will receive a $1.5 million Federal hazard mitigation grant and a $500,000 Aiken County match, bringing the total funds to $2 million, for repair work on the Langley Dam. Repairs will include replacing the spillway and lower gates.
Source:
http://www.aikenstandard.com/article/20160106/AIK0101/160109601/1002/AIK01/aiken-county-officials-to-receive-15m-federal-grant-for-langley-dam-repairs

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