



Daily Open Source Infrastructure Report 28 December 2015

Top Stories

- The owners of Good Neighbor Services Corp., were indicted December 21 for their alleged involvement in a \$7 million insurance fraud and tax evasion scheme that hid the existence of at least 800 hotel workers in California. – *San Diego Union-Tribune* (See item [5](#))
- Oregon officials closed a portion of Highway 42 December 23 for at least a week due to a potential landslide that could spill over the highway. – *Roseburg News-Review* (See item [7](#))
- A December 23 fire at the Rockcastle County jail in Kentucky sent 13 inmates and 2 guards to an area hospital and caused the temporary displacement of about 90 other inmates. – *WKYT 27 Lexington* (See item [17](#))
- A Bahamian man was charged December 22 for allegedly hacking into the email accounts of individuals working in the entertainment and professional sports industries to steal industry and personal information. – *SecurityWeek* (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. *December 24, Associated Press* – (Michigan) **Thousands without power as storms, strong winds cross state.** Consumers Energy reported December 24 that over 82,000 customers in western and northern Michigan lost power due to a severe storm and strong winds December 23 that knocked down trees, utility poles, and power lines.
Source: <http://www.9and10news.com/story/30824732/thousands-without-power-as-storms-strong-winds-cross-state>

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

2. *December 23, New Orleans Times-Picayune* – (Louisiana) **Contractors skipped 10 months of fire inspections at Waterford 3, NRC says.** The U.S. Nuclear Regulatory Commission reported December 23 that contractors at the Entergy-owned Waterford Steam Electric Station, Unit 3 nuclear power plant in Killona failed to conduct required hourly fire inspections and falsified reports for 10 months to prove inspections occurred following a 15-month investigation. Officials also determined that an Entergy supervisor deliberately failed to identify and take corrective actions after being provided with suspected wrongdoing by GCA Contractors.
Source:
http://www.nola.com/environment/index.ssf/2015/12/contractors_skipped_fire_inspe.html

Critical Manufacturing Sector

Nothing to report

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *December 23, Philadelphia Business Journal* – (National) **Local bank pays \$4.3M to settle charges of ‘unfair and deceptive practices.’** The U.S. Federal Deposit Insurance Corporation announced December 23 that The Bankcorp, Inc., will pay \$4.3 million in fines and restitution to settle alleged violations of the Federal Trade Commission Act after authorities found that the bank failed to protect consumers against account errors, failed to provide promised rewards from a debit-card program, and charged deceptive fees on a prepaid card.
Source: <http://www.bizjournals.com/philadelphia/news/2015/12/23/bancorp-ftc-settlement-million-unfair-banking.html>

4. *December 23, Shelby County Reporter* – (Alabama) **Pelham man arrested in connection to \$1 million tax fraud scheme.** The Internal Revenue Service (IRS) announced December 23 that a Birmingham employee was arrested and charged in connection to an alleged stolen identity tax-refund scheme that netted over \$1 million in false claims. Three other co-conspirators were arrested for their alleged roles in the scheme which involved stealing personal identity information from the IRS to create fraudulent tax returns and collecting the stolen refunds.
Source: <http://www.shelbycountyreporter.com/2015/12/23/pelham-man-arrested-in-connection-to-1-million-tax-fraud-scheme/>
5. *December 21, San Diego Union-Tribune* – (California) **Company owners indicted in \$7M hotel-worker fraud case.** The owners of Irvine-based Good Neighbor Services Corp., were indicted December 21 for their alleged involvement in a \$7 million insurance fraud and tax evasion scheme that reportedly hid the existence of at least 800 hotel workers in California in order to avoid paying over \$3.6 million in workers' compensation insurance rates and over \$3.3 million in payroll taxes. The owners, along with 6 accomplices used 12 shell companies to misrepresent the number of employees and the size of payroll in order to defraud insurance providers and the State.
Source: <http://www.sandiegouniontribune.com/news/2015/dec/21/janitor-services-fraud-indictment/>

For additional stories, see items [20](#) and [21](#)

Transportation Systems Sector

6. *December 23, Cortez Journal* – (Colorado) **Seven semis and 12 vehicles crash, shut down U.S. 491.** A portion of U.S. 491 in Cortez, Colorado, was shut down for more than 5 hours December 23 while officials investigated the scene of a multi-vehicle crash involving 7 semi-trucks and 12 other vehicles that sent 3 individuals to the hospital with minor injuries.
Source: <http://www.cortezjournal.com/article/20151223/NEWS01/151229964>
7. *December 23, Roseburg News-Review* – (Oregon) **Landslide closes Highway 42 'for a long time,' says ODOT.** The Oregon Department of Transportation closed Highway 42 at the Coos-Douglas county line December 23 until further notice due to debris from steep hills that may spill over the highway following heavy rainstorms which caused land destabilization. Official reported that the highway could be closed for at least a week.
Source: <http://www.nrtoday.com/news/19803961-113/highway-42-closed-due-to-landslide>
8. *December 23, Macon Telegraph* – (Georgia) **One dead in multiple-vehicle crashes on Interstate 75 in Houston County.** Northbound and southbound lanes of Interstate 75 in Houston County, Georgia, were shut down for several hours December 23 while crews worked to clear debris from a multi-vehicle crash involving at least 2 semi-trucks and 3 other vehicles that left 1 person dead and a second person injured.
Source: <http://www.macon.com/news/local/community/houston->

[peach/article51255545.html](http://www.peach.com/article51255545.html)

9. *December 23, Santa Barbara Noozhawk* – (California) **Woman seriously injured in Highway 101 wreck near El Capitan State Beach.** Railroad tracks by Highway 101 near El Capitan State Beach in Santa Barbara were closed December 23 until further notice following a 2-vehicle crash that sent 1 driver to the hospital with injuries. An inspector will approve the reopening of the railroad tracks following an investigation. Source: http://www.noozhawk.com/article/injuries_reported_in_highway_101_wreck_at_el_capitan
10. *December 23, KGW 8 Portland* – (Oregon) **Warrenton man killed in Highway 30 crash near Clatskanie.** Highway 30 near Clatskanie was closed for approximately 9 hours December 23 following an accident between a semi-truck and a vehicle that left 1 person dead and 2 others injured when the vehicle crossed the center line and struck the oncoming semi-truck sending both into a water-filled ditch next to the highway. Source: <http://www.kgw.com/news/local/deadly-head-on-crash-closes-hwy-30-near-clatskanie/7669272>
11. *December 23, Victor Valley News* – (California) **Portion of Highway 18 shut down following major injury traffic collision.** Eastbound lanes of State 18 Highway in Apple Valley were closed for several hours December 23 after a man was struck and injured while pushing his vehicle along the highway. A second driver also suffered injuries. Source: <http://www.vvng.com/portion-of-highway-18-shut-down-following-major-injury-traffic-collision/>

Food and Agriculture Sector

12. *December 24, WTKR 3 Norfolk* – (Virginia) **Explosion, building collapse at Perdue factory in Accomack County.** A fire official reported December 24 that part of the Perdue Farms factory in Accomack County collapsed after an explosion occurred in the boiler room of the Valley Protein-owned portion of the building. One man was injured and an investigation is ongoing to determine the cause of the explosion. Source: <http://wtkr.com/2015/12/24/explosion-building-collapse-at-purdue-factory-in-accomack-county/>
13. *December 23, U.S. Food and Drug Administration* – (National) **Drug recall – weight loss dietary supplements with undeclared sibutramine and phenolphthalein.** The U.S. Food and Drug Administration announced December 23 that BeeXtreme LLC issued a recall for all lots of its La' Trim Plus, Jenesis, and Oasis dietary supplement products due to misbranding and undeclared drug ingredients including sibutramine and phenolphthalein, which were withdrawn and unapproved for use in U.S. markets. Source: <http://www.fda.gov/Safety/Recalls/ucm478883.htm>
14. *December 23, U.S. Food and Drug Administration* – (National) **American Pure Whey issues allergy alert on undeclared milk and soy in whey protein products.** The U.S.

Food and Drug Administration announced December 23 that American Pure Whey issued a recall for all lots of its 100% Pure Whey Protein Matrix and 100% Pure Whey Protein Isolate after routine inspection revealed that the products contained undeclared milk and soy allergens in the whey ingredient. The products were distributed nationwide and via Internet sales

Source: <http://www.fda.gov/Safety/Recalls/ucm478902.htm>

Water and Wastewater Systems Sector

Nothing to report

Healthcare and Public Health Sector

15. *December 23, KARE 11 Minneapolis* – (Minnesota) **Allina Health clinic improperly disposed of some personal data.** Allina Health is notifying approximately 6,178 patients December 23 that their personal, medical, and insurance information was not properly disposed of after the clinic discovered that the patients' documents were thrown out in a private dumpster and not shredded at the Allina Isles Clinic in Minneapolis. The health care system does not believe that any information was misused.

Source: <http://www.kare11.com/story/news/local/2015/12/23/allina-health-isles-clinic-minneapolis-personal-data/77833710/>

Government Facilities Sector

16. *December 23, Louisville Courier-Journal* – (Kentucky) **False report of gunman disrupts state building.** Employees at the Kentucky State government building in Frankfort were evacuated and sent home December 23 while State police searched the facility following a false report of a gunman in the building. Authorities cleared the scene after nothing suspicious was found.

Source: <http://www.courier-journal.com/story/news/politics/2015/12/23/ky-state-government-building-locked-down/77803432/>

For another story, see item [5](#)

Emergency Services Sector

17. *December 23, WKYT 27 Lexington* – (Kentucky) **Fire inside Rockcastle Co., Ky. jail leads to evacuations, hospitalizations.** A December 23 fire at the Rockcastle County jail in Mt. Vernon, Kentucky, sent 13 inmates and 2 guards to an area hospital to be treated for smoke inhalation and caused the temporary displacement of about 90 other inmates after the fire began following an argument about a television in a jail cell. The jail is closed for repairs until further notice due to extensive smoke and water damage.

Source: <http://www.local8now.com/news/headlines/Fire-inside-Rockcastle-Co-jail-leads-to-evacuations-hospitalizations-363421651.html>

Information Technology Sector

18. *December 23, SecurityWeek* – (International) **Threat group uses new malware to target Russian organizations.** Palo Alto Networks reported that a new threat group, similar to Roaming Tiger operation, has been using a new malware tool dubbed “BBSRAT” to infect devices by using the same command and control (C&C) domains, but deploying different malware variants and separate infrastructure for each of the targeted entities via droppers and downloaders, which creates registry entries for persistence. Once installed on a system, the malware collects data from the infected device and sends it back to a remote server via POST request, allowing attackers to send commands to uninstall or kill the malware, execute a shellcode, start or stop a service, manipulate processes, and execute commands, among other actions.
Source: <http://www.securityweek.com/threat-group-uses-new-malware-target-russian-organizations>

19. *December 23, SecurityWeek* – (International) **Man charged for hacking celebrity emails.** The U.S. Attorney’s Office for the Southern District of New York reported December 22 that a man from the Bahamas was charged for allegedly hacking into the email accounts of 130 individuals working in the entertainment, media, and professional sports industries to steal private files including movie and TV scripts, Social Security numbers, and passport copies via malware and phishing campaigns. The suspect was arrested December 21 after attempting to sell 15 scripts and the personal information of 3 professional athletes and 1 actress for \$80,000.
Source: <http://www.securityweek.com/man-charged-hacking-celebrity-emails>

20. *December 23, SecurityWeek* – (International) **Ramnit botnet returns.** Researchers from IBM Security discovered a new botnet and a new variant of the Ramnit trojan that uses a different command and control (C&C) structure, relies on shorter configuration files, and uses web injections leveraged by other trojans including Dridex, Shifu, and Neverquest to infect banking Web sites from a remote server. The malware is distributed via malvertising campaigns that rely on the Angler exploit kit (EK), but researchers reported that the malware could also be distributed through other infection vectors.
Source: <http://www.securityweek.com/ramnit-botnet-returns>

For another story, see item [21](#)

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

Nothing to report

Commercial Facilities Sector

21. *December 24, SecurityWeek* – (International) **Hyatt Hotels finds malware on payment systems.** Hyatt Hotels Corporation reported December 23 that an investigation is ongoing into a potential breach of its payment processing systems following the discovery of malware on its systems. The company has taken additional steps to strengthen security measures and advised its customers to monitor their payment card statements for any suspicious activity.
Source: <http://www.securityweek.com/hyatt-hotels-finds-malware-payment-systems>

22. *December 24, KUSA 9 Denver* – (Colorado) **About 80 passengers evacuated after ski lift breaks in Aspen.** Aspen Skiing Co. officials reported December 24 that about 80 passengers were safely evacuated from the Tiehack Express lift in Aspen December 23 after the machine went offline due to an electrical error.
Source: <http://www.9news.com/story/news/local/2015/12/23/about-80-passengers-evacuated-after-ski-lift-breaks-in-aspen/77856632/>

For another story, see item [5](#)

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.