Homeland Security

Daily Open Source Infrastructure Report
04 May 2015

Top Stories

- The U.S. Department of Energy reported April 30 that the agency will pay New Mexico $73 million in projects for violations that led to a radiation leak in February 2014. – *Reuters* (See item **1**)

- The U.S. Department of Justice announced a $20 million pilot program May 1 to extend the use of police body cameras in order to help enhance transparency, advance public safety, and promote accountability. – *NBC News* (See item **16**)

- Federal authorities announced April 29 that 13 current and former law enforcement officers from North Carolina and Virginia were charged in connection to allegedly protecting cocaine and heroin shipments along the East Coast. – *WTVD 11 Durham* (See item **17**)

- AT&T and its former subsidiary, Southern New England Telephone agreed to pay a combined $10.9 million in penalties April 29 to resolve an investigation by the U.S. Federal Communications Commission for overbilling the FCC's Lifeline program. – *U.S. Federal Communications Commission* (See item **22**)

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

See item **1**

Chemical Industry Sector

Nothing to report

Nuclear Reactors, Materials, and Waste Sector

1. *May 1, Reuters* – (New Mexico) **U.S. Government to pay New Mexico $73 million over radiation leak.** U.S. Department of Energy officials reported April 30 that the agency will pay New Mexico $73 million in projects in and around the Waste Isolation Pilot Plant in Carlsbad for violations at the plant and at the Los Alamos National Laboratory that led to a radiation leak in February 2014. Projects include road improvements, nuclear waste transportation routes, storm-water management upgrades, and the construction of an emergency operations center.
Source: http://in.reuters.com/article/2015/05/01/us-usa-new-mexico-nuclear-idINKBN0NM2X020150501

2. *April 30, Hartsville Messenger* – (South Carolina) **Duke Energy to clean up coal ash at Robinson Nuclear Plant.** Duke Energy announced April 30 that the company will dig up 4.2 million tons of coal ash in the areas surrounding the Robinson Nuclear Plant near Hartsville and relocate it in a new, Class 3 lined landfill on site. The South Carolina Department of Health and Environmental Control cited Duke Energy in 2014 after detecting levels of arsenic up to 100 times the State standard for drinking water in groundwater near Lake Robinson.
Source: http://www.scnow.com/messenger/article_d52b9464-ef3a-11e4-88e0-6ffc0afcf8c3.html

Critical Manufacturing Sector

3. *April 30, U.S. Department of Labor* – (Ohio) **Lack of proper safety controls leads to loss of worker's 3 fingers in metal press at stamping company, inspectors find.** The Occupational Safety and Health Administration cited Shiloh Industries Inc., April 30 for 7 serious violations at its Wellington Stamping plant in Ohio, including failing to train workers in energy control procedures, posing an amputation hazard. Proposed fines total $49,000.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEA

SES&p_id=27879

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

4. *April 30, KESQ 42 Palm Springs* – (National) **2 men arrested with hundreds of fraudulent credit cards.** Two individuals were arrested April 29 in Palm Desert for burglary, fraud, identity theft, and possession of stolen property after authorities discovered hundreds of manufactured credit cards, purchased gift cards, and stolen clothing and electronics from several local businesses in a rental car. Investigators allege the pair racked up tens of thousands of dollars in fraudulent charges in the area with stolen credit card numbers from victims across the U.S.
Source: http://www.kesq.com/news/2-men-arrested-with-hundreds-of-fraudulent-credit-cards/32671160

For another story, see item **20**

Transportation Systems Sector

5. *May 1, St. Louis Post-Dispatch* – (Missouri) **Pedestrian fatally struck after crash on I-270 in Creve Coeur.** Northbound lanes of Interstate 270 in Creve Coeur were closed for 5 hours May 1 due to a man being fatally struck while crossing the northbound lanes by foot after crashing his vehicle into a median. Authorities are investigating the incident.
Source: http://www.stltoday.com/news/local/crime-and-courts/pedestrian-hit-and-killed-while-trying-to-cross-i-/article_bbe49a0c-eed8-57ef-b61e-f3b39a9ebc12.html

6. *May 1, WNBC 4 New York City* – (New Jersey) **Several critically injured after alleged drunk driver strikes NJ Transit bus: Police source.** A driver, passenger, six bus passengers, and the bus driver were transported to an area hospital after a car struck a New Jersey Transit bus at Central Avenue and South Eighth Street May 1.
Source: http://www.nbcnewyork.com/news/local/Car-Crash-NJ-Transit-Bus-Newark-Critical-Injuries-302108851.html

7. *April 30, New York Daily News* – (New York) **Plane makes emergency landing at LaGuardia Airport after striking bird.** An Envoy Air flight headed to Detroit returned to LaGuardia Airport in New York for an emergency landing shortly after takeoff when its left flap slammed into a bird April 30.

Source: http://www.nydailynews.com/new-york/plane-emergency-landing-laguardia-bird-strike-article-1.2205603

For another story, see item **1**

Food and Agriculture Sector

8. *April 30, Associated Press* – (Iowa) **Bird flu losses likely to top 20M with new cases in Iowa.** Iowa agriculture officials reported April 30 that 5 additional Iowa farms are likely affected by an ongoing H5N2 avian flu outbreak, including an egg-laying operation with 5.5 million chickens. Minnesota officials also reported 3 new presumed cases across the State.
Source: http://www.wxow.com/story/28946581/bird-flu-losses-likely-to-top-20m-with-new-cases-in-iowa

9. *April 30, U.S. Department of Agriculture* – (National) **Ohanyan's Bastirma & Soujouk, Co. recalls sausage products due to misbranding and an undeclared allergen.** The Food Safety and Inspection Service (FSIS) announced April 30 that Ohanyan's Bastirma & Soujouk Co., issued a recall for about 150,291 pounds of its Dried Beef Sausage products due to misbranding and undeclared soy lecithin. The recall was initiated after FSIS inspectors found that the establishment did not declare canola oil spray that was applied on the interior of tubs used during the manufacturing process.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-072-2015-release

Water and Wastewater Systems Sector

10. *May 1, Glenwood Springs Post Independent* – (Colorado) **Water near No Name Trail contaminated.** Garfield County officials reported May 1 that it posted signs warning residents to avoid coming into contact with standing water near No Name Trail #2068 (Jess Weaver Trail) after tests confirmed the presence of E. coli following a small wastewater discharge that occurred along County Road 129.
Source: http://www.postindependent.com/news/16136216-113/water-near-no-name-trail-contaminated

For another story, see item **1**

Healthcare and Public Health Sector

11. *April 30, WYMT 57 Hazard* – (Tennessee) **Health information for more than 1,700**

Holston Valley Medical Center patients found in recycling bin. Wellmont Health Systems officials reported April 30 that the protected health information of 1,726 Holston Valley Medical Center patients were found in a recycling bin at Steel Creek Park in Bristol, Tennessee, March 1. The information contained notes created by a former nurse who provided care for patients between 1998 and 2007, and authorities do not believe any personal information was compromised.
Source: http://www.wkyt.com/wymt/home/headlines/Health-information-for-more-than-1700-Holston-Valley-Medical-Center-patients-found-in-recycling-bin-301824091.html

12. *April 30, Associated Press* – (Massachusetts) **Partners HealthCare notifies 3,300 patients of email breach.** Boston-based Partners HealthCare announced April 30 that it notified approximately 3,300 patients of a security breach that allowed hackers to access medical and personal information, including Social Security numbers, following a November 2014 incident where a group of employees received phishing emails that tricked their targets to provide password information or to click on malicious links.
Source: http://abcnews.go.com/Technology/wireStory/partners-healthcare-notifies-3300-patients-email-breach-30716877

[Return to top]

Government Facilities Sector

13. *May 1, WGGB 40 Springfield/WSHM 3 Springfield* – (Massachusetts) **Palmer public schools closed Friday to "calm things down" following threats.** Nearly all Palmer public schools in Massachusetts were closed May 1 following a series of threats made towards several schools in the district April 29-April 30. Police reported that four of the five suspects who made the threats were identified.
Source: http://www.wfsb.com/story/28942563/threat-reported-against-comverse-middle-school-in-palmer

14. *April 30, University of California, Berkeley* – (California) **Campus announces data breach.** Officials at the University of California, Berkeley announced April 30 that about 260 undergraduate students and some former students, as well as approximately 290 parents and other individuals may have had their personal and financial information, including Social Security numbers, accessed in a computer data breach when an unauthorized user gained access to a campus Web server in December 2014 and February 2015. Campus officials removed the server from the network after discovering the breach March 14, and continue to investigate.
Source: https://newscenter.berkeley.edu/2015/04/30/campus-announces-data-breach/

15. *April 30, WLEX 18 Lexington* – (Kentucky) **Children taken to hospital after Scott Co. school bus crash.** Eight Scott County elementary students were transported to an area hospital as a precaution after a school bus was rear-ended by a vehicle on U.S. 25 near Double Culvert Road April 30.
Source: http://www.lex18.com/story/28945294/scott-co-school-bus-involved-in-accident

Emergency Services Sector

16. *May 1, NBC News* – (National) **Police body cams: DOJ unveils $20M program to expand use.** The U.S. Department of Justice announced a $20 million pilot program May 1 to extend the use of police body cameras in order to help enhance transparency, advance public safety, and promote accountability.
Source: http://www.nbcnews.com/storyline/baltimore-unrest/body-worn-cameras-get-20m-federal-pilot-amid-baltimore-protests-n351721

17. *May 1, WTVD 11 Durham* – (North Carolina; Virginia) **13 current and former North Carolina and Virginia law enforcement officers indicted.** Federal authorities announced April 29 that 13 current and former law enforcement officers from North Carolina and Virginia, along with 2 civilians, were charged in connection to allegedly protecting cocaine and heroin shipments along the East Coast. The officers and civilians were charged with allegedly collaborating to distribute controlled substances and conspire to use firearms in relation to drug trafficking offenses.
Source: http://abc11.com/news/13-current-and-former-law-enforcement-officers-indicted/688835/

Information Technology Sector

18. *May 1, Securityweek* – (International) **Security bug in ICANN portals exploited to access user data.** The Internet Corporation for Assigned Names and Numbers (ICANN) released April 30 initial findings from an investigation revealing that a vulnerability in two of the organizations generic top-level domain (gTLD) portals had resulted in the exposure of 330 advanced search result records pertaining to 96 applicants and 21 registry operators since April 2013. The organization plans to contact both the affected users and those who exploited the vulnerability to access the records.
Source: http://www.securityweek.com/security-bug-icann-portals-exploited-access-user-data

19. *May 1, Help Net Security* – (International) **Unnoticed for years, malware turned Linux and BSD servers into spamming machines.** Security researchers at ESET discovered that servers running BSD and Linux operating systems (OS) worldwide have been targeted for the past 5 years by a group that compromised systems via a backdoor trojan that would use a commercial automated e-mail distribution system to send out anonymous emails.
Source: http://www.net-security.org/malware_news.php?id=3030

20. *May 1, Threatpost* – (International) **Dyre banking trojan jumps out of sandbox.** Security researchers at Seculert discovered a new strain of the Dyre banking trojan, called Dyreza, that evades detection by checking for the number of processor cores

running on an infected machine, and terminating itself if there is only one. The researchers also noted that the new strain changed to a new user agent and included other minor updates to avoid signature-based detection products.
Source: https://threatpost.com/dyre-banking-trojan-jumps-out-of-sandbox/112533

21. *April 30, Threatpost* – (International) **MySQL bug can strip SSL protection from connections.** Researchers at Duo Security identified a serious vulnerability in how versions of Oracle's MySQL database product handle requests for secure connections, in which an attacker could use a man-in-the-middle (MitM) attack to force an unencrypted connection and intercept unencrypted queries from the client to the database. In this scenario, the attack could occur regardless of whether or not the server is toggled to require secure socket layer (SSL).
Source: https://threatpost.com/mysql-bug-can-strip-ssl-protection-from-connections/112513

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

[Return to top]

Communications Sector

22. *April 29, U.S. Federal Communications Commission* – (National) **AT&T and SNET to pay $10.9 million for overbilling Lifeline program.** AT&T and its former subsidiary Southern New England Telephone (SNET) agreed to pay a combined $10.9 million in penalties April 29 to resolve an investigation by the U.S. Federal Communications Commission (FCC) for overbilling the FCC's Lifeline program by providing service to landline customers without recertifying eligibility within the time limit set.
Source: https://www.fcc.gov/document/att-and-snet-pay-109-million-overbilling-lifeline-program

[Return to top]

Commercial Facilities Sector

23. *May 1, KRIV 26 Houston* – (Texas) **Three-alarm fire destroys Seabrook hotel.** The Hampton Inn hotel in Seabrook suffered a partial roof collapse during a 3-alarm fire that through the structure May 1. Guests and staff were evacuated without incident.
Source: http://www.myfoxhouston.com/story/28952356/three-alarm-fire-destroys-seabrook-hotel

24. *May 1, WUSA 9 Washington, D.C.* – (Washington, D.C.) **Parking garage collapses at**

Watergate Hotel. One person was injured May 1 when at least 2 floors of a parking garage at the Watergate Hotel in the Northwest quadrant of Washington, D.C., suffered a "pancake collapse". The incident remains under investigation.
Source: http://www.wusa9.com/story/news/local/dc/2015/05/01/collapse-2-floors-watergate-hotel/26696867/

25. *May 1, Livingston Press* – (Michigan) **Police give OK to return to Green Oak Costco after bomb threat.** About 300 customers and staff were evacuated from a Costco store in Green Oak April 30 after a handwritten bomb threat was found in a restroom at the business. Police searched and cleared the store to reopen about 2 hours later after no suspicious device was found.
Source: http://www.livingstondaily.com/story/news/crime/2015/04/30/costco-bomb-threat-green-oak-evacuation/26646553/

26. *May 1, WPXI 11 Pittsburgh* – (Pennsylvania) **Residents, business owners lose everything in Vandergrift blaze.** An April 30 fire in Vandergrift, Pennsylvania, burned through a restaurant and at least 5 apartment units, displacing 12 residents. Officials ruled the fire accidental.
Source: http://www.wpxi.com/news/news/local/breaking-firefighters-battling-intense-blaze-apart/nk6Wk/

27. *April 30, WSB 2 Atlanta* – (Georgia) **Hotel shut down after suspected meth lab explosion.** The Cartersville North Inn and Suites motel in Georgia was ordered closed by State fire officials April 30 following a suspected meth lab explosion inside a guest room that caused damage to the structure. The motel will remain closed until repairs are made and HAZMAT crews clear all hazardous materials from the scene.
Source: http://www.wsbtv.com/news/news/local/crews-investigate-explosion-cartersville-north-inn/nk6Cw/

[Return to top]

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.