Daily Open Source Infrastructure Report
09 May 2016

Top Stories

- Two men were arrested and charged May 5 after detectives caught them using counterfeit credit cards to make fraudulent purchases at the Dadeland Mall and stores throughout Miami-Dade County. – *WTVJ 6 Miami* (See item **4**)
- Service on the Washington Metropolitan Area Transit Authority's Orange and Blue lines was restored May 6 after service was suspended at four stations in Washington, D.C. May 5 following two track fires. – *WRC 4 Washington, D.C.* (See item **7**)
- A painter at Hartwood Farm in Willistown Township, Pennsylvania, was charged May 5 for allegedly embezzling $927,100 from the farm by depositing stolen checks into various personal accounts. – *WPVI 6 Philadelphia* (See item **11**)
- A 4-alarm warehouse fire May 5 at Custom Packaging and Filling Company in west Houston prompted a shelter-in-place for residents and the evacuation of 730 people from Spring Branch Elementary School. – *Houston Chronicle* (See item **26**)

Fast Jump Menu

Energy Sector

Nothing to report

Chemical Industry Sector

See item **26**

Nuclear Reactors, Materials, and Waste Sector

1. *May 5, KING 5 Seattle* – (Washington) **Record number of Hanford workers sickened by toxic vapors.** Officials from the U.S. Department of Energy reported May 4 that a total of 47 workers at the Hanford Nuclear Site have sought medical evaluations since April 28 after suffering symptoms due to chemical vapor releases or as a precautionary measure after workers smelled odors and experienced symptoms consistent with chemical vapor exposure. Officials stated chemical vapor releases at the site come from underground nuclear waste storage tanks that vent the gasses without warning.
   Source: http://www.king5.com/news/local/investigations/record-number-of-hanford-workers-sickened-by-toxic-vapors-at-nuclear-site/172394029

Critical Manufacturing Sector

2. *May 5, U.S. Consumer Product Safety Commission* – (National) **BRP recalls side-by-side off-road vehicles due to loss of steering control and crash hazard (recall alert).** Bombardier Recreational Products & Vehicles (BRP) issued a recall May 5 for approximately 10,600 of its model year 2013 Can-Am Commander side-by-side off-road vehicles equipped with Dynamic Power Steering (DPS) due to a faulty steering coupling that can strip on the rack and pinion assembly and result in a loss of steering, thereby increasing the risk of a crash after the firm received 29 incident reports. The vehicles were sold at Can-Am dealers nationwide.
   Source: http://www.cpsc.gov/en/Recalls/Recall-Alerts/2016/BRP-Recalls-Side-By-Side-Off-Road-Vehicles/

Defense Industrial Base Sector

Nothing to report

Financial Services Sector

3. *May 6, SecurityWeek* – (International) **New trojan targets banks in US, Mexico.** Researchers from Zscaler discovered that a new information stealer trojan which leverages legitimate tools to target online banking users in the U.S. and Mexico is delivered via the “curp.pdf.exe” installer served on several compromised Web sites which downloads a main payload file, a Fiddler dynamic link library (DLL) file, and a Json.Net DLL file on a victim’s device to collect system information and send it back to the command and control (C&C) server, to parse the server’s response and save the

information in an extensible markup language (XML) file, and to intercept Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS) connections and redirect users to a malicious Web site masked as a bank's legitimate domain.
Source: http://www.securityweek.com/new-trojan-targets-banks-us-mexico

4. *May 5, WTVJ 6 Miami* – (Florida) **Pair arrested in counterfeit credit card scheme: MDPD.** Two men were arrested and charged May 5 after detectives witnessed the duo using counterfeit credit cards to make fraudulent purchases at the Dadeland Mall and stores throughout Miami-Dade County. Authorities stated a subsequent search of one of the suspects' vehicles revealed 192 counterfeit credit cards.
Source: http://www.nbcmiami.com/news/local/Pair-Arrested-in-Counterfeit-Credit-Card-Scheme-MDPD-378339951.html

5. *May 5, Chicago Sun Times* – (Illinois) **Chicago financial adviser pleads guilty to $4.2M fraud.** The operator of a Chicago-based investment firm, D.J. Mosier and Associates pleaded guilty May 5 to defrauding 9 clients out of more than $4.2 million by persuading them to invest in phony "Chicago Anticipatory Notes" debt securities. The financial adviser cashed the investors' checks into her personal bank account and used the money for personal expenses, and to make bogus interest payments to previous clients.
Source: http://chicago.suntimes.com/news/chicago-financial-adviser-pleads-guilty-to-4-2m-fraud/

Transportation Systems Sector

6. *May 6, WSOC 9 Charlotte* – (North Carolina) **Big rig crash spills 50K pounds of potatoes across I-77.** One lane of Interstate 77 in Charlotte, North Carolina, was reopened 6 hours after a section of the interstate was closed May 6 while crews worked to clear 50,000 pounds of potatoes that spilled from a semi-truck after the driver fell asleep and crashed into the guard rail.
Source: http://www.wsoctv.com/news/local/violent-tractor-trailer-crash-spills-thousands-of-potatoes-across-i-77/264345110

7. *May 6, WRC 4 Washington, D.C.* – (Washington, D.C.) **Metro service restored after fire closes 2 stations.** Service on the Washington Metropolitan Area Transit Authority's Orange and Blue lines between Eastern Market and L'Enfant Plaza and between Capitol South and Federal Center SW was restored May 6 after service was suspended May 5 when two separate fires shut down a section of the track, prompting the closures. Officials stated that one fire was sparked by a porcelain insulator which will be replaced with fiberglass parts, while the other was due to debris on the track.
Source: http://www.nbcwashington.com/traffic/transit/Metro-Trains-on-3-Lines-Delayed-by-Track-Problem-378320681.html

8. *May 6, KDVR 31 Denver* – (Colorado) **I-76 closed in both directions after semitruck splits through another.** Authorities are investigating a May 6 accident involving two semi-trucks and a vehicle that closed Interstate 76 west in Wiggins, Colorado for

several hours and sent three drivers to a nearby hospital with injuries. Crews worked to clear the scene after paint supplies and other materials being hauled by a semi-truck spilled onto the roadway.
Source: http://kdvr.com/2016/05/06/i-76-closed-in-both-directions-west-of-wiggins-after-semitrucks-collide/

9. *May 5, Charleston Gazette-Mail* – (West Virginia) **Coal train derails in eastern Kanawha County.** Seven cars on a CSX Transportation train transporting coal derailed near the intersection of Cabin Creek Road and Ronda Road in West Virginia May 5, prompting the closure of Cabin Creek Road after four of the derailed cars overturned, blocking the road. Crews estimated that the removal of the wrecked portion of the train could take 2 – 3 days.
Source: http://www.wvgazettemail.com/news/20160505/coal-train-derails-in-eastern-kanawha-county

Food and Agriculture Sector

10. *May 5, U.S. Department of Labor* – (Kansas) **OSHA cites The Scoular Company for exposing workers to grain dust, fall hazards at Kansas site.** The Occupational Safety and Health Administration cited The Scoular Company with one repeat and four serious safety violations May 2 after an investigation at the Tribute, Kansas facility revealed that the company failed to implement housekeeping procedures to prevent grain dust accumulation and dust explosions, and failed to install guardrails on ladder way openings and open-sided work platforms, among other violations. Proposed penalties total $47,300.
Source:
https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=31743

11. *May 5, WPVI 6 Philadelphia* – (Pennsylvania) **Bryn Mawr painter accused of stealing $900K from Chester County farm.** A painter at Hartwood Farm in Willistown Township, Pennsylvania, was charged May 5 for allegedly embezzling $927,100 from the farm after he stole 148 blank checks, forged the property owner's signature, and deposited the fraudulent checks into various personal accounts from May 2014-February 2016. Officials stated the man used the money for personal expenses.
Source: http://6abc.com/news/painter-accused-of-stealing-$900k-from-pa-farm/1325168/

12. *May 5, U.S. Food and Drug Administration* – (National) **Pita Pal Foods, LP recalls Corn Relish Salad, Texas Caviar Salad, Mediterranean 3 Bean Salad and Chipotle Quinoa Salad because of possible health risk.** Pita Pal Foods, LP issued a recall May 5 for its Corn Relish Salad, Texas Caviar Salad, Mediterranean 3 Bean Salad, and Chipotle Quinoa Salad products due to a potential Listeria monocytogenes contamination after one of the company's ingredient suppliers, CRF Frozen Foods, issued a voluntary recall for the specific lot of frozen corn used in manufacturing the salad products. Pita Pal Foods, LP destroyed the specific lot of corn and no illnesses have been reported in connection with the products which were shipped to retail stores

and food service distributors in eight States.
Source: http://www.fda.gov/Safety/Recalls/ucm499568.htm

13. *May 5, U.S. Department of Agriculture* – (Iowa; Nebraska) **The Grey Plume Provisions, LLC recalls charcuterie meat products produced without benefit of inspection.** The Grey Plume Provisions, LLC issued a recall May 5 for approximately 471 pounds of its charcuterie meat products sold in 9 variations after the Iowa Department of Agriculture discovered that the products were produced, packaged, and distributed without the benefit of Federal inspection. There have been no confirmed reports of adverse reactions and the products were shipped to wholesale locations in Iowa and Nebraska.
Source: http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2016/recall-036-2016-release

Water and Wastewater Systems Sector

14. *May 6, Associated Press* – (North Dakota) **Work underway on $25.7M flood wall at Minot water plant.** Crews began work on a $25.7 million project to enhance flood protection for Minot's water treatment plant May 6, which includes the installation of a 1,720-foot-long flood wall along the Souris River. The flood wall is part of a larger flood protection plan for Minot due to a June 2011 incident where the river swelled with snowmelt and rain and spilled its banks, causing an estimated $700 million in damage.
Source: http://www.wahpetondailynews.com/work-underway-on-m-flood-wall-at-minot-water-plant/article_76f0049c-12cb-11e6-9750-d3456bacd0ab.html

Healthcare and Public Health Sector

15. *May 5, Fresno Bee* – (California) **Saint Agnes Medical Center victim of data breach.** Officials at the Saint Agnes Medical Center in California reported May 5 that hackers obtained W-2 information of 2,800 individuals employed by the hospital in 2015 via a May 2 phishing attack. The hospital stated that no patient information was compromised and that its systems were not breached.
Source: http://www.fresnobee.com/news/local/crime/article76002977.html

16. *May 5, Associated Press* – (National) **FDA brings e-cigarettes under Federal authority; will restrict youth access within 90 days.** The U.S. Food and Drug Administration released new rules May 5 that will limit e-cigarette sales to minors, require new health warnings, and require manufacturers to obtain Federal permission to continue marketing all e-cigarettes launched since 2007. The new measures will go into effect by August.
Source: http://www.foxnews.com/health/2016/05/05/fda-brings-e-cigarettes-under-federal-authority.html

Government Facilities Sector

17. *May 6, Asheville Citizen-Times* – (North Carolina) **Authorities investigate bomb**

threats made to WNC counties. The Jackson County Courthouse, Cherokee Tribal Courts, and Swain County Courthouse in western North Carolina were all evacuated and closed for the remainder of May 5 due to a bomb threat. An investigation into the threat is ongoing.
Source: http://www.citizen-times.com/story/news/local/2016/05/05/bomb-threats-made-wnc-counties/83976264/

18. *May 5, Salem News* – (Massachusetts) **6 children injured in school bus crash.** Six Nathaniel Bowditch Elementary School students and a driver were transported to area hospitals with injuries after a vehicle struck a school bus at an intersection in Salem, Massachusetts, May 5.
Source: http://www.salemnews.com/news/local_news/children-injured-in-school-bus-crash/article_3026cbb7-d450-5dfc-b1c7-bb984a850653.html

19. *May 5, KUSA 9 Denver* – (Colorado) **CDOT employee stole contractors' personal information.** A Colorado Department of Transportation (CDOT) spokesperson announced May 5 that the personal information of hundreds of CDOT contractors may have been compromised after a data breach involving a CDOT employee who had access to a database for Emerging Small Business (ESB) and Disadvantaged Business Enterprise (DBE) which contained confidential information. Authorities stated that the businesses potentially impacted by the breach submitted information to CDOT in order to qualify for ESB and DBE programs.
Source: http://www.9news.com/news/cdot-employee-stole-contractors-personal-information/175000302

For another story, see item **26**

Emergency Services Sector

See item **26**

Information Technology Sector

20. *May 6, Help Net Security* – (International) **Android trojan pesters victims, won't take no for an answer.** Avast researchers determined that an information-stealing Android trojan that is inadvertently downloaded by users, begins its infection after an icon is installed in the launcher in the name of a fake app which launches a dialog box that asks the user to grant it admin rights and blocks further access. Users can remove the trojan by powering down the phone and restoring it to factory settings or uninstalling the app.
Source: https://www.helpnetsecurity.com/2016/05/06/android-trojan-pesters-victims/

21. *May 6, Threatpost* – (International) **New security flaw found in Lenovo Solution Center software.** Trustwave SpiderLabs reported a new vulnerability in Lenovo's Solution Center software which is tied to the software's backend and can allow an attacker with local network access to a PC to execute arbitrary code and elevate privileges. The company updated a previous security advisory disclosing the additional

vulnerability and released a fix addressing the vulnerability.
Source: https://threatpost.com/new-security-flaw-found-in-lenovo-solution-center-software/117896/

22. *May 5, Softpedia* – (International) **Ransomware infections grew 14 percent in early 2016, April the worst month.** Kaspersky, Enigma Software Group, and the FBI issued a warning to companies about the increase in ransomware infections following reports of at least 2,900 new ransomware variants, representing a 14 percent increase in Quarter 1 of 2016. Researchers also found a significant increase in the number of attacks during April.
Source: http://news.softpedia.com/news/ransomware-infections-grew-14-percent-in-early-2016-april-the-worst-month-503743.shtml

23. *May 5, Softpedia* – (International) **New Attack on WordPress sites redirects traffic to malicious URLs.** Security researchers from Sucuri reported that hackers were continuously leveraging vulnerabilities in older WordPress versions or WordPress plugins by altering the Web sites' main theme's header.php file via 12 lines of obfuscated code to redirect users to malicious Web sites. In addition, Joomla Web sites were seen with a similar malicious code in the administrator/includes/help.php file.
Source: http://news.softpedia.com/news/new-attack-on-wordpress-sites-redirects-traffic-to-malicious-urls-503740.shtml

24. *May 5, SecurityWeek* – (International) **Qualcomm software flaw exposes Android user data.** Security researchers from FireEye discovered Qualcomm Technologies, Inc., open source software package and devices running Android 5.0 Lollipop and earlier versions were plagued with an information disclosure vulnerability that could allow a malicious application to access user information as long as the application has the "ACCESS_NETWORK_STATE" permission. Qualcomm issued security updates patching the vulnerability.
Source: http://www.securityweek.com/qualcomm-software-flaw-exposes-android-user-data

25. *May 5, SecurityWeek* – (International) **Adobe issues pre-patch advisory for Reader, Acrobat.** Adobe issued a pre-patch advisory stating that it will release patches for its PDF Reader and Acrobat software products May 10, which will address critical vulnerabilities on the Microsoft Windows and Apple Mac operating system (OS) X platforms.
Source: http://www.securityweek.com/adobe-issues-pre-patch-advisory-reader-acrobat

For another story, see item **3**

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

26. *May 6, Houston Chronicle* – (Texas) **Four-alarm sends plumes of smoke across Houston, runoff into creeks.** A 4-alarm warehouse fire May 5 at Custom Packaging and Filling Company in west Houston prompted a shelter-in-place for residents, evacuated 730 people from the Spring Branch Elementary School and surrounding businesses, and prompted more than 170 firefighters to remain on site containing the incident after the fire began in a garage area of a nearby home. Officials warned residents to avoid the Spring Branch Creek and nearby ditches and culverts after chemical additives from firefighters' efforts flowed into the creek.
Source: http://www.chron.com/news/houston-texas/houston/article/Three-alarm-fire-burns-at-business-in-NW-Houston-7395178.php

27. *May 5, KSTU 13 Salt Lake City* – (Florida) **Neighbors help others escape overnight apartment fire.** The Palencia Apartments in Carrollwood, Florida, sustained extensive damage May 5 due to an early-morning fire that displaced 48 residents. The cause of the fire is under investigation.
Source: http://www.fox13news.com/news/local-news/137200608-story

28. *May 5, Salt Lake Tribune* – (Utah) **Fire displaces 50 people at Millcreek apartment complex.** A May 5 fire at the Monaco Apartments in Millcreek displaced 50 residents and damaged at least 24 units in 2 buildings after the blaze was inadvertently ignited by a cigarette on a third-floor balcony and spread to an adjacent building. Fire officials shut down surrounding roads due to the incident.
Source: http://www.sltrib.com/home/3860505-155/crews-fighting-3-alarm-fire-in-millcreek

29. *May 5, Chicago Sun-Times* – (Illinois) **Firefighters battle extra-alarm blaze at Harvey strip mall.** A strip mall was deemed a total loss following an extra-alarm fire that broke out in the basement of the strip mall on East 154th Street in south Harvey, Illinois, May 5.
Source: http://chicago.suntimes.com/news/firefighters-battle-extra-alarm-blaze-at-harvey-store/

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