Homeland Security

Daily Open Source Infrastructure Report 22 October 2012

Top Stories

- Kolon Industries Inc. and several of its executives and employees were indicted for allegedly engaging in a multi-year campaign to steal trade secrets related to DuPont’s Kevlar para-aramid fiber and Teijin Limited’s Twaron para-aramid fiber, officials announced October 18. – *U.S. Department of Justice* (See item **2**)
- HSBC blamed a distributed denial-of-service (DDoS) attack for the downtime of many of its Web sites worldwide October 18. – *The Register* (See item **8**)
- An offshore remittance company called Caribbean Transfers financed a complex money-laundering ring that moved more than $30 million in stolen Medicare money from south Florida into Cuba’s banking system, federal authorities announced October 17. – *Miami Herald* (See item **28**)
- Kaspersky Labs is developing a secure operating system for industrial control systems, the company’s chairman and CEO said October 16. The new system aims to protect complex industrial systems that have become the target of a variety of high-profile cyberweapons. – *IDG News Service* (See item **45**)

Fast Jump Menu

Energy Sector

1. *October 18, Associated Press* – (Iowa) **Fuel spill in Des Moines River traced to generator.** Officials said a diesel fuel spill discovered October 18 in the Des Moines River in downtown Des Moines was traced to a rooftop generator at the Iowa Events Center. The Iowa Department of Natural Resources (DNR) said about 2,500 gallons of diesel flowed down a roof drain from a standby generator on the roof of Hy-Vee Hall. It flowed into a storm drain that led to the river. Cleanup crews placed absorbent booms across the river. A DNR spokesman said there was no danger to the city's drinking water supply.
   Source: http://qctimes.com/news/state-and-regional/iowa/fuel-spill-in-des-moines-river-traced-to-generator/article_6525c9fd-9f46-540e-8caa-75480437cbf8.html

[Return to top]

Chemical Industry Sector

2. *October 18, U.S. Department of Justice* – (National; International) **Top executives at Kolon Industries indicted for stealing DuPont's Kevlar trade secrets.** Kolon Industries Inc. and several of its executives and employees were indicted for allegedly engaging in a multi-year campaign to steal trade secrets related to DuPont's Kevlar para-aramid fiber and Teijin Limited's Twaron para-aramid fiber, the U.S. Department of Justice announced October 18. The indictment seeks forfeiture of at least $225 million in proceeds from the alleged thefts. "Kolon is accused of engaging in a massive industrial espionage campaign that allowed it to bring Heracron quickly to the market and compete directly with Kevlar," said a U.S. attorney. Headquartered in Seoul, South Korea, Kolon was indicted by a grand jury in Richmond, Virginia. The indictment charges Kolon with one count of conspiring to convert trade secrets, four counts of theft of trade secrets, and one count of obstruction of justice. Kevlar is produced by E.I. du Pont de Nemours and Company (DuPont), one of the largest chemical companies in the United States.
   Source: http://www.fbi.gov/richmond/press-releases/2012/top-executives-at-kolon-industries-indicted-for-stealing-duponts-kevlar-trade-secrets

For another story, see item **34**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

3. *October 19, Brattleboro Reformer* – (Vermont) **Yankee: Tritium response finished.** Test results from a drinking water well at Brattleboro, Vermont's Yankee nuclear power plant meant the plant's response to the discovery in January 2010 of a leak of tritiated water is officially over, said a Yankee spokesman, the Brattleboro Reformer reported October 19. September 17, Yankee technicians sampled a decommissioned drinking water well connected to the plant's construction office

building (COB). Samples were analyzed by both the Vermont Department of Health (DOH) and a laboratory contracted by Yankee. “Test results from both the Health Department Laboratory and its contract laboratory report that neither tritium nor gamma-emitting radioactive materials were detected in the COB well samples,” stated a press release from DOH. “Tritium results ... were all less than the detection limit for all three samples.” No tritium was ever detected in drinking water wells either on or offsite from the leak.
Source: http://www.reformer.com/localnews/ci_21806474/yankee-tritium-response-finished

4. *October 17, ScienceDaily* – (International) **Cosmic rays could assist in healing Fukushima’s nuclear scar.** Researchers from Los Alamos National Laboratory have devised a method to use cosmic rays, or muons, to gather detailed information from inside the damaged cores of the Fukushima Daiichi nuclear reactors, ScienceDaily reported October 17. A paper in Physical Review Letters stated that researchers compared two methods for using cosmic-ray radiography to gather images of nuclear material within the core of a reactor similar to Fukushima Daiichi Reactor No. 1. The team found that Los Alamos’ scattering method for cosmic-ray radiography was far superior to the traditional transmission method for capturing high-resolution image data of potentially damaged nuclear material. Muon radiography uses muons to create images of the objects that the muons penetrate. The process is analogous to an X-ray image, except muons are produced naturally and do not damage the materials they contact. Los Alamos researchers found that by placing a pair of muon detectors in front of and behind an object, the scientists could gather detailed images. The method works particularly well with highly interfering materials such as uranium. Due to the fact the muon scattering angle increases with atomic number, core materials within a reactor show up more clearly than surrounding objects.
   Source: http://www.sciencedaily.com/releases/2012/10/121017132025.htm

[Return to top]

Critical Manufacturing Sector

5. *October 19, Associated Press* – (National) **Feds probe complaints that Jeep Patriots stall.** U.S. government safety regulators are investigating complaints that engines on Jeep Patriot SUVs can stall without warning at highway speeds, the Associated Press reported October 19. The problem caused one crash in which two people were hurt, according to documents posted on the National Highway Traffic Safety Administration (NHTSA) Web site. The investigation affects about 112,000 Patriots from the 2011 and 2012 model years that were sold in the United States by Chrysler Group LLC, the maker of Jeeps, as well as 18,000 that were sold in Canada. NHTSA said that it received a dozen complaints about stalling. Ten of the incidents occurred while the Jeeps were going 65 miles per hour or faster. In eight cases the Patriots could not be restarted and had to be towed.
   Source: http://www.wavy.com/dpp/news/us_news/Feds-investigate-Jeep-Patriot-stalling-problem_63475413

[Return to top]

Defense Industrial Base Sector

See item **31**

[Return to top]

Banking and Finance Sector

6. *October 19, Associated Press* – (Florida) **3rd person guilty in $39M Fla. mortgage fraud.** A third person pleaded guilty in federal court to taking part in a $39 million mortgage fraud scheme involving a Fort Lauderdale, Florida condominium, the Associated Press reported October 19. A man from New York City pleaded guilty to mail and wire fraud conspiracy charges. Prosecutors said the man and six other people recruited buyers for units at the condominium. They used false mortgage applications and misrepresented the buyers' credit standing in order to get the loans. The group then diverted a portion of the mortgage proceeds for their own use.
   Source: http://www.sfgate.com/news/crime/article/3rd-person-guilty-in-39M-Fla-mortgage-fraud-3963466.php

7. *October 19, Associated Press* – (Pennsylvania) **Pa. developer charged with bank fraud.** A developer from Gladwyne, Pennsylvania, was charged with bank fraud for using false information to get more than $13 million in loans from two banks. The U.S. attorney's office in Philadelphia said October 18 that the developer was charged with bank and wire fraud and making false statements to banks. A U.S. attorney said the developer induced Boyertown-based National Penn Bank in 2007 and the former Wilmington Bank in 2008 to lend him $13 million on the basis of fraudulent securities statements. His attorney said her client had already admitted wrongdoing.
   Source: http://www.wfmj.com/story/19861077/pa-developer-charged-with-bank-fraud

8. *October 19, The Register* – (International) **HSBC Web sites fell in DDoS attack last night, bank admits.** HSBC blamed a distributed denial-of-service (DDoS) attack for the downtime of many of its Web sites worldwide October 18. Readers told The Register that they were unable to reach the HSBC UK and First Direct Web sites, leaving them unable to carry out Internet banking services. The problems lasted for around 7 hours. In a statement, HSBC said attacks affected customers worldwide, and reassured clients that sensitive account data was not exposed by the attack. Security researchers analyzing the earlier attacks quickly came to the conclusion that they were largely powered by botnet networks of malware-infected PCs. An EMEA Solutions architect team lead at Arbor Networks said: "Recent attacks have used what we call multi-vector attacks, attacks which utilize a combination of volumetric, and application layer attack vectors. What we are seeing here are TCP, UDP, and ICMP packet floods combined HTTP, HTTPS, and DNS application layer attacks."
   Source: http://www.theregister.co.uk/2012/10/19/hsbc_ddos/

9. *October 19, KNSD 7 San Diego* – (California) **'Chubby Bandit' sought in robbery series.** FBI investigators said the man known as the 'Chubby Bandit' is responsible for five bank robberies and one attempted robbery in San Diego County, KNSD 7 San Diego reported October 19. Investigators said the first robbery happened October 9 at a US Bank branch in Poway. October 11 a similar suspect description was reported in the robbery at Chase Bank in Carlsbad. Officials said the same suspect attempted to rob a Chase Bank October 13 in Solana Beach. Then he robbed a Wells Fargo Bank in Encinitas October 15, and a US Bank in Carlsbad October 16. October 18, the suspect is believed to have robbed a bank located inside a Rancho Bernardo grocery store. The suspect used a demand note and made verbal demands, and also verbally threatened and gestured to have a gun during his robberies officials said.
Source: http://www.nbcsandiego.com/news/local/Bank-Robbery-Chubby-Bandit-San-Diego-FBI-Suspect-174791171.html

10. *October 19, Associated Press* – (North Dakota; Arizona) **Arizona pair due in ND court on bank fraud charges.** Two executives from a defunct Arizona mortgage lender were due in a North Dakota federal court October 19 to hear charges against them alleging that they swindled Bismarck, North Dakota-based BNC National Bank out of at least $26 million. The two men are charged with conspiracy to commit bank fraud and wire fraud, and court records indicated they might enter pleas during the hearing. One was the CEO of American Mortgage Specialists Inc. (AMS) and the other was the company's vice president in charge of lending operations. Authorities said AMS defrauded BNC by providing it with false financial statements and other information about the status of loans the bank had financed. A printout obtained by a BNC employee in April 2010 showed that few loans at AMS remained to be sold, according to court documents. "The printout revealed that approximately $565,000 of loans remained to be sold, rather than the approximately $27 million of loans which were shown in BNC records as being held for sale to investors," a federal affidavit reads. "BNC ceased funding the loans, and AMS closed its operations."
Source: http://www.sfgate.com/news/article/Arizona-pair-due-in-ND-court-on-bank-fraud-charges-3963573.php

11. *October 18, Reuters* – (International) **Ally Financial latest US bank to face cyber attacks.** October 18, Ally Financial became the latest U.S. financial institution to face a cyberattack. Bank of America, Wells Fargo, and other banks in recent weeks have suffered so-called distributed denial-of-service (DDoS) attacks in which hackers use a high volume of incoming traffic to delay or disrupt customer Web sites. Regional bank BB&T and credit card issuer Capital One confirmed disruptions earlier the week of October 15. A spokeswoman for Ally said the bank was investigating the "unusual traffic" on its Web site. Banks have stressed that customer accounts and information was not at risk, but the attacks have highlighted the growing threat from hackers against U.S. infrastructure.
Source: http://www.nbcnews.com/technology/technolog/ally-financial-latest-us-bank-face-cyber-attacks-1C6557410

12. *October 18, Bloomberg News* – (New York; International) **Hedge fund manager pleads guilty to forex fraud.** A hedge fund manager who fled the United States after

being accused of swindling clients admitted to running a scheme to cheat investors out of $5 million, Bloomberg News reported October 18. The man pleaded guilty to wire fraud before a U.S. District Judge in Brooklyn, New York, prosecutors said in an emailed statement. The man controlled foreign-currency hedge funds Century Maxim Fund Inc. and AJR Capital Inc., and had faced mail-fraud, wire-fraud, and money-laundering charges. The man was indicted in 2006 after fleeing the country in 2005. He traveled to Mexico, Panama, and Poland, where he assumed a false identity using a fraudulent Russian passport. He was arrested in Poland in May 2011 and extradited to the United States in August. He also operated an investment scheme while in Panama. He stole from more than 100 clients who gave him $5 million in 2004 and 2005 to invest, prosecutors said. He gambled more than $3 million at a casino in Connecticut, according to prosecutors. He told the investors he would invest their money in the stock market and foreign currency exchange market. He falsely said that he had a history of profitable trading and that he would use a "stop-loss" mechanism to ensure that no trade would lose more than 3 percent, the government said. Formerly of Staten Island, New York, the manger fled the United States while on supervised release after leaving prison in April 2003 for a conviction in a foreign-exchange scheme, according to prosecutors. He pleaded guilty in that case after being extradited from France.
Source: http://www.businessweek.com/news/2012-10-18/hedge-fund-manager-efrosman-pleads-guilty-to-forex-fraud

13. *October 18, U.S. Federal Bureau of Investigation* – (Texas) **Former Houston attorney pleads guilty to $7.8M investment scheme.** A former attorney residing in Houston pleaded guilty to one count of wire fraud in connection with his investment fraud scheme that victimized more than 20 investors of approximately $7.8 million, a U.S. attorney announced October 18. During the past 10 years, the attorney held himself out to friends and potential investors as being involved in the real estate investment business. While he did conduct some legitimate business activity during this time period, a substantial portion of the funds he solicited were simply part of a Ponzi scheme he was operating in an effort to satisfy old debts and to fund his personal lifestyle. In acknowledging his criminal conduct, the attorney admitted to using a variety of ploys to perpetuate his Ponzi scheme, all of which involved falsely representing to investors the existence or nature of various real estate investment opportunities, accepting funds from investors under such false pretenses, and then using the investor funds in a manner other than as represented to investors.
Source: http://www.loansafe.org/former-houston-attorney-pleads-guilty-to-7-8m-investment-scheme

14. *October 18, Salt Lake Tribune* – (Utah) **FBI offers $5,000 reward for 'Bundled Up Bandit'.** Federal and local Utah law enforcement agencies are offering a $5,000 reward for information leading to the arrest of a serial bank robber known as the "Bundled Up Bandit," the Salt Lake Tribune reported October 18. A FBI spokeswoman said that the suspect, known for wearing multiple layers of concealing clothing, a knit cap, and sunglasses, is believed to have held up three Utah banks in the past month. The most recent robbery happened October 17 when the suspect walked into a Bank of the West in Cottonwood Heights. Just moments after the bank had opened, he handed a note to a teller demanding cash — and claimed to have both a gun and a bomb. The teller handed

over an unspecified amount of cash and the suspect fled on foot.
Source: http://www.sltrib.com/sltrib/news/55107400-78/bank-fbi-suspect-cash.html.csp

15. *October 17, Bank Systems and Technology* – (National) **One in four customers are card fraud victims, study finds.** A new study looking at the behavior and concerns of customers worldwide concerning card fraud was released October 17 by payments solutions provider ACI Worldwide and the Aite Group, a research firm. The 2012 fraud report, titled “Global Consumers React to Fraud: Beware Back of Wallet,” found that 27 percent of global consumers had been hit by credit card fraud over the past 5 years. Many of those who experienced fraud turned to using cash, checks, or other cards more after receiving a replacement card. The study found that 46 percent of customers who received a replacement card because of a data breach or other fraud activity used the card less than before. The study asked more than 5,200 customers in more than 17 countries around the globe if they had experienced card fraud and how that had changed their consumer behavior. The percentage of respondents who had experienced fraud in the last 5 years stayed consistent with the 2011 report findings, but there was a sharp increase in the number of respondents who had experienced fraud more than once in the last 5 years. This year 14 percent of the respondents had been victimized by fraudsters multiple times, compared to only 6 percent last year.
Source: http://www.banktech.com/one-in-four-customers-are-card-fraud-vic/240009173

[Return to top]

Transportation Sector

16. *October 19, Associated Press* – (Oklahoma) **Dust storm shuts down interstate in northern Okla.** A massive dust storm swirling reddish-brown clouds over northern Oklahoma triggered a multi-vehicle accident along a major interstate October 18, forcing police to shut down part of the heavily traveled roadway amid near blackout conditions. A Blackwell police chief said nine people were injured, but there were no fatalities. The crashes involved nearly three dozen cars and tractor-trailers. State transportation workers were called in to close the highway between U.S. 60 and Oklahoma 11, an 8-mile stretch of the cross-country roadway. Choking dust suspended on strong wind gusts shrouded Interstate 35, which links Dallas and Oklahoma City to Kansas City, Missouri. A dispatcher with the Kay County Sheriff’s Office said, “In this area alone, the dirt is blowing because we’ve been in a drought. I think from the drought everything’s so dry and the wind is high.” The stretch of closed roadway reopened after crews cleaned up debris and waited for winds to die down, an Oklahoma Department of Transportation spokesman said.
Source: http://www.cbsnews.com/8301-505245_162-57535868/dust-storm-shuts-down-interstate-in-northern-okla/

17. *October 19, WISH 8 Indianapolis* – (Indiana) **Kids hurt in school bus crash near Frankfort.** Emergency officials said dozens of children were being taken to a hospital after a school bus crashed October 19 near Frankfort, Indiana. The bus involved was for Clinton Prairie schools. The crash happened at Clinton County Road 450 West and

Manson-Colfax Road, emergency officials said. There were no other vehicles involved in the crash. Three children were taken via ambulance to an area hospital. The driver and 23 other children were taken to the hospital in another school bus. The bus was carrying students in kindergarten through 12th grade.
Source: http://www.wishtv.com/dpp/news/local/north_central/kids-hurt-in-school-bus-crash-near-frankfort

18. *October 19, Associated Press* – (Louisiana) **18-wheelers crash closing I-10 westbound near Lafayette.** State police said one person was killed after an 18-wheeler crashed at the foot of the Atchafalaya Basin Bridge at Henderson, Louisiana, prompting the closure of Interstate 10 westbound October 18. A trooper said an 18-wheeler traveling east crossed the median and struck another 18-wheeler traveling west. He said one of the 18-wheelers was carrying drilling mud that caught fire as a result of the crash. Westbound I-10 remained closed October 19.
Source: http://www.wwltv.com/news/18-wheelers-crash-closing-I-10-westbound-near-Lafayette-174939771.html

19. *October 17, Fierce Government* – (National) **FAA needs data policy changes to better address accidents, finds GAO.** The Federal Aviation Administration (FAA) needs to undertake steps to reduce accident rates and improve related data collection, says a report from the Government Accountability Office (GAO). In the report dated October 4, auditors note that most general aviation accidents are a result of pilot error. The FAA bases some its accident-reduction goals and efforts on defined accident rates and annual flight hours, but the GAO warns that "shortcomings in flight activity data" will make it difficult to achieve reductions in fatality rates among the riskier segments. The GAO report says the FAA needs more specific performance measurements for each program in its accident reduction strategy to better determine if goals are being met or if more actions are needed, which is important because current operations "may not meet the overall goal by 2018." This goal and others fall under several FAA initiatives including the renewal of the General Aviation Joint Steering Committee and the implementation of the Flight Standards Service's 5-year strategy, which involves a series of efforts around risk management, outreach, training, and safety promotion. To strengthen measurements and better evaluate program goals, the GAO suggests the FAA explore new ways to collect flight hours more often with methods that "minimize the impact on the general aviation community." This would allow the FAA to establish accident-reduction goals for each individual industry segment, making better use of its existing data and making the goals easier to manage and achieve.
Source: http://www.fiercegovernment.com/story/faa-needs-data-policy-changes-better-address-accidents-finds-gao/2012-10-17

[Return to top]

Postal and Shipping Sector

20. *October 18, Elk Grove Patch* – (California) **Suspects allegedly ambush UPS truck, attempt to steal video games.** A UPS driver making deliveries in Elk Grove, California, was attacked and hit in the face with a rock October 16. According to an Elk

Grove Police Department crime log, a car pulled up behind the truck and flashed its headlights. The driver pulled over and began speaking with the driver. A passenger from the car then climbed into the UPS truck, hit the driver in the face with a rock, and demanded he hand over boxes from GameStop. The second suspect fought with the driver and was able to rip open two boxes. He exited the truck and fled the scene in his car.
Source: http://elkgrove.patch.com/articles/suspects-allegedly-ambush-ups-truck-attempt-to-steal-video-games

[Return to top]

Agriculture and Food Sector

21. *October 18, Associated Press* – (National) **Smucker's Uncrustables sold to schools recalled.** J.M. Smucker Co. of Orrville, Ohio, used peanut butter that was produced by Sunland Inc. in "limited production runs" of 72-count bulk packs of the sandwiches that went to schools under the National School Lunch Program, a Smucker's spokeswoman said in an email October 18. The company found no problems with the peanut butter, which was supplied by the U.S. Department of Agriculture, or the finished products after routine tests. However, the spokeswoman said Smucker's recently notified school customers that they should check if they have any sandwiches from the recalled lots; the recalled sandwiches have either expired or will expire soon. She said she did not immediately know how many sandwiches were involved.
Source: http://vitals.nbcnews.com/_news/2012/10/18/14542685-smuckers-uncrustables-sold-to-schools-recalled?lite#__utma=238145375.289694522.1348658399.1350558446.1350644341.19&__utmb=238145375.1.10.1350644341&__utmc=238145375&__utmx=-&__utmz=238145375.1350644341.1

[Return to top]

Water Sector

22. *October 18, Lehigh Valley Morning Call* – (Pennsylvania) **3-county drinking-water cancer warning is fake, State says.** A post office bulletin telling residents to beware of cancer-causing drinking water in Carbon, Schuylkill, and Luzerne counties in Pennsylvania is a hoax, the Pennsylvania Department of Environmental Protection (DEP) said October 18. The bulletin, posted in the McAdoo Post Office in Kline township, Schuylkill county, claimed the drinking water in at least 10 communities in those counties was linked to polycythemia vera, a form of blood cancer, the DEP said. "Currently, DEP knows of no drinking water contamination issues associated with any of the public water systems in those areas," the DEP said in a news release. "Additionally, the agency knows of no environmental link between PV [the disease] and drinking water in Carbon, Luzerne,and Schuylkill counties." The McAdoo Post Office bulletin labeled itself an "official public notice," but the DEP said it did not appear to have come from any official agency. The bulletin urged residents to buy water filters.

Source: http://www.mcall.com/news/breaking/mc-c-carbon-schuylkill-water-cancer-hoax-20121018,0,5877487.story

23. *October 18, Minneapolis Star Tribune* – (Minnesota) **Drought brings pleas to cut back water use.** With rivers and rainfall approaching record low levels, Minnesota State officials said October 18 they want homeowners to eliminate "nonessential" water use, such as lawn watering and car washing, and have told farmers to abide strictly by irrigation permits. In parts of the State, some residential wells have run dry or had flow reduced by commercial and residential neighbors, said the deputy director of Ecological and Water Resources at the Department of Natural Resources (DNR). Continued lack of rain could prompt the DNR, under terms of a drought action plan, to require specific water conservation targets for users, particularly cities. In recent weeks it suspended 50 permits for surface water use by businesses, golf courses, and parks departments across the State, though many have backup water sources. The weekly update of the U.S. Drought Monitor noted a gradual retreat of drought conditions nationally, but an area of extreme drought broadened across southwest Minnesota. Nearly half the State was classed as experiencing extreme or severe drought, with a wide patch of northwestern Minnesota remaining in the extreme category.
Source: http://www.startribune.com/local/174786211.html?refer=y

24. *October 18, WFOR 4 Miami* – (Florida) **Boil water order issued for Margate, parts of Coconut Creek.** Officials in Margate and Coconut Creek, Florida warned their residents to boil their drinking water after well water tests came back positive for traces of fecal matter. The well in question was removed from service and further tests would be performed to determine when the well water will be safe to drink. City officials recommend bringing water to a rolling boil, then continue to boil the water for one minute, before cooling and drinking. Officials encouraged residents to use boiled or bottled water for drinking, making ice, preparing food, and washing dishes until tests on the contaminated water show levels have returned to normal.
Source: http://miami.cbslocal.com/2012/10/18/boil-water-order-issued-for-margate-parts-of-coconut-creek/

25. *October 18, WPMT 43 York* – (Pennsylvania) **Boil water advisory for some Lancaster City water customers.** The Northwest Lancaster County Authority (NWLCA) informed customers October 17 on Fruitville Pike, Lititz Road, and Sun Valley Drive in Lancaster, Pennsylvania, that they experienced a loss of positive water pressure due to a loss of water supply from Lancaster City Water. A loss of positive water pressure signaled the existence of conditions that could allow contamination to enter the distribution system through back-flow by back-pressure or back-siphonage. As a result, there was an increased chance that the water may contain disease-causing organisms. Residents were told not to drink the water without boiling it first. Boiled or bottled water should be used for drinking, making ice, brushing teeth, washing dishes, and food preparation until further notice.
Source: http://www.fox43.com/news/wpmt-boil-water-advisory-for-some-lancaster-city-water-customers,0,7417356.story

For another story, see item **1**

[Return to top]

Public Health and Healthcare Sector

26. *October 18, Philadelphia Inquirer* – (Pennsylvania) **Man who posed as chiropractor gets six years for fraud.** A federal judge October 18 sentenced a Philadelphia man to 6 years in prison for posing as a chiropractor and trying to bilk $1.4 million from the insurer Independence Blue Cross. In late 2008, the Philadelphia man agreed to buy the Oasis Holistic Healing Village from its retiring owner and said he planned to hire a licensed professional chiropractor to continue offering services, court filings showed. Instead, he posed as a chiropractor himself and examined patients. Using the former owner's medical provider number, he submitted more than $1.4 million in claims for insurance repayment. In 2009, Independence Blue Cross received four times the amount of what the former owner had billed the previous year, and more than it received from any single chiropractor nationwide, prosecutors said. The insurer paid $285,000. Besides recognizing the inflated billings, the company started fielding complaints from patients about the practice. One patient told investigators he or she never visited the office, even though the insurer was billed for treating the patient 50 times. FBI agents confronted the Philadelphia man in the spring of 2011, and he admitted to the billings. A grand jury later indicted him on more than 100 counts of health care-related fraud.
Source: http://www.philly.com/philly/news/breaking/174858061.html

27. *October 18, Ft. Lauderdale Sun-Sentinel* – (Florida) **Halfway house operator gets four years for Medicare fraud.** The owner of the Florida corporation New Way Recover Inc., that operated several halfway houses, was sentenced October 17 for his role in a $205 million Medicare fraud scheme. Between April 2004 and September 2010, he and others received kickback payments in exchange for referring Medicare beneficiaries for medically unnecessary treatments. American Therapeutic Corporation never provided the medical services that were charged to Medicare, court records showed. He received more than 4 years in federal prison, plus 3 years' probation, and was ordered to pay $2,413,675 in restitution with his co-conspirators.
Source: http://articles.sun-sentinel.com/2012-10-18/news/fl-halfway-house-sentence-20121018_1_medicare-fraud-health-care-fraud-american-therapeutic-corporation

28. *October 18, Miami Herald* – (Florida; International) **Laundering ring moved Medicare money to Cuba bank, US officials say.** An offshore remittance company called Caribbean Transfers financed a complex money-laundering ring that moved more than $30 million in stolen Medicare money from south Florida into Cuba's banking system, federal authorities said October 17. The revelation surfaced in the widening case of a now-convicted check-cashing store owner who was first believed to be at the center of the money-laundering scheme. It marked the first time that investigators traced tainted Medicare proceeds to Cuba's State-controlled bank. Prosecutors filed new conspiracy charges against the founder of the Caribbean-based company, who is at large, and two Miami-Dade County men suspected of defrauding the taxpayer-funded Medicare program. The latter defendants are accused of laundering their Medicare profits through the convicted check-cashing store owner, who did

business with Caribbean Transfers. The new information about Caribbean Transfers, which prosecutors said is licensed by the Cuban government, was disclosed during the bond hearing of one of the Miami-Dade County men October 17. The U.S. attorney's office said it has no evidence that the Cuban government was involved in the laundering scheme, and Cuban officials denied any involvement.
Source: http://www.bellinghamherald.com/2012/10/18/2734149/laundering-ring-moved-medicare.html

29. *October 18, Knoxville News-Sentinel* – (Tennessee) **Blount hospital laptop stolen with 27K patients' personal info.** Blount Memorial Hospital began notifying 27,000 patients whose personal information was compromised after the theft of an employee's laptop computer during a burglary at the staffer's Knoxville, Tennessee, residence August 25. Notifications began October 18 after IT personnel finished verifying whose information was uploaded to the laptop during its most recent backup. The password-protected laptop contained registration records from Blount Heart Consultants on approximately 22,000 patients, including their names, dates of birth, responsible party names, addresses, physician names, and billing information. The laptop also held records on approximately 5,000 additional patients, including the above information along with their Social Security numbers and other non-medical data. The theft is being investigated by the Knoxville Police Department.
Source: http://www.knoxnews.com/news/2012/oct/18/blount-hospital-laptop-stolen-with-27k-patients/

30. *October 17, New York Times* – (National) **Lapses at big drug factories add to shortages and danger.** The New York Times reported October 17 that recent quality lapses at big drug companies show that contamination and shoddy practices extend well beyond the loosely regulated compounding pharmacies that have attracted attention because of their link to an outbreak of meningitis. In the last three years, six of the major manufacturers of sterile injectable drugs were warned by the Food and Drug Administration about serious violations of manufacturing rules. Four of them have closed factories or significantly slowed production to fix the problems. Nearly a third of the industry's manufacturing capacity is offline because of quality issues, according to a Congressional report. Several industry observers and former plant employees said the recent quality issues were troubling and that manufacturers had been reluctant to fix problems because stopping production was simply too costly in a business where profits were driven by volume.
Source: http://www.nytimes.com/2012/10/18/business/drug-makers-stalled-in-a-cycle-of-quality-lapses-and-shortages.html?hp&_r=1&

[Return to top]

Government Facilities Sector

31. *October 19, Associated Press* – (California) **Calif. Navy official pleads to bribery charges.** October 18, federal prosecutors said a Navy official agreed to plead guilty to involvement in a bribery and corruption scheme at Naval Air Station North Island in California. A U.S. Attorney said the plea is subject to a judge's approval. In the plea,

the Navy official admitted accepting bribes along with other Navy officials who were given more than $1 million in cash and gifts. In return, defense contractors in Poway received millions of dollars in defense business. The Navy official was employed in a unit that obtained funding within the government for aircraft maintenance and repair.
Source: http://www.militarytimes.com/news/2012/10/ap-navy-north-island-official-pleads-bribery-charges-101912/

32. *October 19, Lorain Morning Journal* – (Ohio) **Elyria school safety system shuts down phone, Internet.** Schools in Elyria, Ohio, lost phone lines and Internet access October 18. Dust on a sensor set off a chain reaction that disabled computerized systems for the majority of the school day. While the district could still dial 9-1-1 in the event of an emergency, a non-existing emergency perceived by a state-of-the-art safety system crippled most land line communications in the district. The outage affected all of the district's buildings, except for the middle school, which had yet to be updated to a new phone system. Problems started when dust set off an advanced smoke alarm system's sensor tucked into the peak of the bell tower at the old Washington building at the new high school. The system, seeing the speck, believed it was detecting smoke and reacted as programmed, the superintendent said. It set off a series of silent alarms and shut down systems in the building to protect them from possible smoke or heat damage. It took the school's air conditioning and heating offline to avoid spreading "smoke" throughout the building. With the air conditioning off, the school's server room — responsible for keeping the district's network and voice over Internet protocol phone lines operating — heated up quickly, reaching as high as 140 degrees, the superintendent said. The outage lasted for nearly 8 hours. No damage was done to any of the school's systems, he said.
Source:
http://morningjournal.com/articles/2012/10/19/news/doc5080c79c57b68919820920.txt?viewmode=fullstory

33. *October 18, Lubbock Daily Toreador* – (Texas) **Texas State receives bomb threat Thursday morning via email.** According to a news release from the University News Service at Texas State University October 18 a Texas State University Houston-area admissions counselor, who works from home, received a bomb threat via email. The admissions counselor notified supervisors, and supervisors notified the University Police Department (UPD). The bomb threat targeted Texas State's Admissions building so the university evacuated and closed the building. Students received notification of the bomb threat and classes continued with no interruption. UPD, in consultation with the Austin Bomb Squad, and FBI created an 800-foot safety perimeter, consequently causing two residence halls — San Jacinto Hall and Tower Hall — to evacuate and close. UPD canceled the emergency alert October 18. San Jacinto and Tower Hall were reopened, and the Admissions building was closed for the remainder of the day. Classes remained on normal schedule.
Source: http://www.dailytoreador.com/news/article_cd6fbe74-19a1-11e2-a904-0019bb30f31a.html

34. *October 18, U.S. Environmental Protection Agency* – (Maryland) **Maryland Air National Guard settles hazardous waste violations at Baltimore facility.** The U.S. Environmental Protection Agency (EPA) announced October 18 that the Maryland Air National Guard (MDANG), 175th Wing, agreed to pay a $75,000 penalty to settle alleged violations of hazardous waste regulations at its Baltimore facility. The consent agreement resolves alleged violations discovered in an April 2011 inspection. According to the EPA, MDANG stored hazardous waste for more than 90 days without a Resource Conservation and Recovery Act (RCRA) hazardous waste permit or interim status, failed to provide annual hazardous waste training to some of its employees for a 3-year period, and violated RCRA rules on labeling and recordkeeping. The wastes involved in these alleged violations included lubricants, paints, sealants, cleaning solutions, and adhesive wastes. These wastes are hazardous because they exhibited the characteristics of being ignitable, corrosive, or toxic due to chromium, methyl ethyl ketone, or other compounds.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/d0e836342e4230a185257a9b005f8445!OpenDocument

For more stories, see items **17** and **21**

[Return to top]

Emergency Services Sector

35. *October 18, San Bernardino Sun* – (California) **Fumes spark evacuations from Loma Linda University Medical Center.** Dozens of patients were evacuated from Loma Linda University Medical Center in California October 18, after fumes spread through the emergency room and other portions of the hospital, fire officials said. A spray adhesive being used by a construction crew repairing the roof of the hospital seeped into the ventilation system, sending adhesive fumes into the emergency room and portions of the first through third floors, the Loma Linda fire marshal said. Thirty-eight people were evacuated from the emergency room. Patients who did not need to be taken elsewhere were transferred to unaffected areas of the hospital. After pushing fresh air through the air system and using fans to clear the fumes out of the building, the emergency room was reopened roughly 6 hours later.
Source: http://www.sbsun.com/ci_21802601/loma-linda-university-medical-center-emergency-room-evacuated

36. *October 18, Associated Press* – (National; International) **Calif., other States take part in earthquake drill.** Millions of Americans preparing to survive an earthquake ducked under tables and covered their heads October 18, as part of the annual “Great ShakeOut” drill. Organizers said some 14 million people, including 9.3 million in California, signed up to participate. Schoolchildren, hospital workers, elected officials, and others from San Francisco to Washington, D.C participated. The drill was held in some western and southeastern States, as well as Guam, Puerto Rico, and parts of Canada and Italy.

Source: http://www.charlotteobserver.com/2012/10/18/3606129/calif-other-states-take-part-in.html

37. *October 18, Associated Press* – (California) **Cellmate held as suspect in death of inmate at maximum security prison near Sacramento.** California prison officials said an inmate at a maximum security prison was killed and that his cellmate was being held as a suspect. The inmate was found dead October 17 at California State Prison in Folsom. October 18, a prison spokesman said the dead inmate and his cellmate were the only ones in the cell.
Source:
http://www.therepublic.com/view/story/4620a6e29e1149c28cdaee4e3e86164c/CA--California-Prison-Death

[Return to top]

Information Technology Sector

38. *October 19, ZDNet* – (International) **'Major interruption' at GitHub as attackers launch DDoS.** Code sharing repository GitHub was hit by a distributed denial-of-service (DDoS) attack, causing major disruptions to its services. GitHub began investigating the issue at 1:05 p.m. PST, and by 1:33 p.m. PST, alerted its community to the attack. By 3:52 p.m. PST, it rectified the issue and reported everything was operating normally. GitHub wrote on its status page that it was looking into implementing "additional mitigation strategies to harden ourselves against future attacks." GitHub also experienced a series of DDoS attacks in February, and like those previous attacks, no one is claiming responsibility for this latest disruption.
Source: http://www.zdnet.com/major-interruption-at-github-as-attackers-launch-ddos-7000006030/

39. *October 19, Softpedia* – (International) **US election-related news planted in malicious airline emails to avoid spam filters.** Malicious emails purporting to come from airline companies are not new. They inform the recipient that a ticket has been purchased using their credit card and point to an attached file for additional details. However, the more recent airline scams come with a twist. In an effort to evade spam filters, the cyber criminals started adding legitimate-looking text to the end of the email. This text would look highly suspicious if they appeared at the end of an airline notification, so the crooks set the font to white to make it invisible. Although the recipient does not see anything, spam filters do, and considering that the topic is related to the upcoming U.S. presidential elections, the anti-spam mechanisms might view them as legitimate and let the email pass through to the user's inbox.
Source: http://news.softpedia.com/news/US-Election-Related-News-Planted-in-Malicious-Airline-Emails-to-Avoid-Spam-Filters-300721.shtml

40. *October 19, Softpedia* – (International) **MUSTAN malware avoids infecting certain files to hide its presence.** Trend Micro experts analyzed a piece of malware called PE_MUSTAN.A, a threat believed to be connected to the old WORM_MORTO.SM. The malicious element is interesting not just because of the way it spreads from one

computer to the other, but also because of the mechanisms it uses to stay hidden. Researchers found that MUSTAN spreads throughout networks via the Remote Desktop Protocol by brute forcing weak passwords. “If certain user name and password combinations are in use, the malware will be able to gain access and start infecting files on the new system. This behavior is similar to WORM_MORTO,” a Trend Micro senior threat response engineer explained. Once it infects a computer, the malware uses all the available drives, network shares, and the Remote Desktop Protocol in order to spread. It infects all .exe files, except for the ones located in folders such as “Common Files,” “Internet Explorer,” “Messenger,” “Microsoft,” “Movie Maker,” “Outlook,” “qq,” “RECYCLER,” “System Volume Information,” “windows,” and “winnt.” It is believed the .exe files from these folders would cause application crashes if they were infected, and thus reveal the malware’s presence. That is why MUSTAN avoids compromising the files from these locations.
Source: http://news.softpedia.com/news/MUSTAN-Malware-Avoids-Infecting-Certain-Files-to-Hide-Its-Presence-300650.shtml

41. *October 19, Softpedia* – (International) **Fake Lookout Mobile Security update steals files from Android users.** Lookout recently warned customers about an application on Google Play that mimicked an update for their Android application. Experts from TrustGo analyzed the threat after the malicious element was removed from the online store. According to researchers, once installed on an Android smartphone, the malware — Trojan!FakeLookout.A — was capable of stealing SMS and MMS messages and uploading them to a remote server via FTP. The trojan also sent its controllers a list of the files present on the device’s SD card. Based on this list, cyber criminals could upload specific files. TrustGo experts accessed the FTP server on which the stolen files were stored and they found not only SMS messages but also some video files. The server, apparently located somewhere in Colorado, also hosts a malicious Web Site designed to drop a backdoor trojan. This Web Site serves the malware to Windows users and also to ones running Mac OS and Linux operating systems. Depending on the OS, the site drops a different trojan. The malware found on Google Play is just a part of a larger attack. Judging by the complexity of the campaign, it is likely the cybercriminals who orchestrate it will somehow resurrect the Android trojan and disguise it as another legitimate-looking app.
Source: http://news.softpedia.com/news/Fake-Lookout-Mobile-Security-Update-Steals-Files-from-Android-Users-300603.shtml

42. *October 19, The H* – (International) **Encryption found insufficient in many Android apps.** Researchers discovered catastrophic conditions when analyzing Android applications that use encryption: more than 1,000 of the 13,500 most popular Android apps showed signs of a flawed and insecure implementation of the SSL/TLS encryption protocol. Tests performed on 100 selected apps confirmed that 41 of them were vulnerable to known attacks. The researchers harvested users’ bank and credit card details as well as the access tokens for their Facebook, Twitter, email accounts, and messaging services. The vulnerabilities the researchers found can be divided into 2 categories: 20 apps simply accepted any certificate, while the other 21 did check whether the certificate carried a valid signature, but did not verify whether it was issued to the correct name. This allowed the security experts to fool the anti-virus software

with a valid certificate for its own server.
Source: http://www.h-online.com/security/news/item/Encryption-found-insufficient-in-many-Android-apps-1732847.html

43. *October 19, The H* – (International) **Microsoft and Secunia warn of FFMpeg vulnerabilities.** Microsoft provided details of several critical vulnerabilities in older versions of FFmpeg's open source video codec tools and libraries; these could allow an attacker to execute arbitrary code on a system by getting users to open a specially crafted media file. This would execute the malicious code with the same permissions as the user. Another issue reported by Secunia could have the same effect. For the Microsoft flaws, all versions of FFmpeg up to and including 0.10 are vulnerable, while for the Secunia issue, versions up to and including 0.11.2 are affected. The Microsoft-discovered vulnerabilities are present in the libavcodec library which suffers from memory corruption when parsing ASF, QuickTime, and Windows Media Video files.
Source: http://www.h-online.com/security/news/item/Microsoft-and-Secunia-warn-of-FFMpeg-vulnerabilities-1732963.html

44. *October 18, BBC News* – (International) **French hacker 'admits app fraud' in Amiens.** A hacker admitted to spreading a virus via smartphone applications that defrauded thousands of victims after he was arrested in the city of Amiens in northern France. Prosecutors said he stole tiny sums from 17,000 people, amassing about $650,000 since 2011. Working from his parents' home, he snared victims with free downloads designed to look like original apps, they said. However, in the background, the apps worked to steal money via hidden transactions. It appears smartphones that use Google software were the most susceptible, according to a BBC correspondent in Paris. Once the fake applications were downloaded, the virus sent a text message without the user's knowledge to a premium-rate number the hacker set up. There were also programs that sent him the log-on codes for gaming and gambling Web sites to which the victims subscribed.
Source: http://www.bbc.co.uk/news/world-europe-19994944

45. *October 17, IDG News Service* – (International) **Kaspersky to develop a secure OS for industrial control.** Russian security firm Kaspersky Lab is developing a secure operating system for industrial control systems (ICS), the company's chairman and CEO said October 16. The new system aims to protect complex industrial systems that have become the target of a variety of high-profile cyberweapons such as Stuxnet, Duqu, Flame, and Gauss. Most control systems were not created with security in mind, which is the reason that most information exchange protocols in supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLCs) require no user identification or authorization. Kaspersky plans to build the operating system with the help of ICS vendors and users and use entirely new code. To be fully secure, the core must be fully verified to not permit vulnerabilities or dual-purpose code. The kernel also needs to contain a very bare minimum of code, and that means that as much code as possible, including drivers, needs to be controlled by the core and be executed with low-level access rights, according to the analysis by the Lab.
Source:

http://www.computerworld.com/s/article/9232483/Kaspersky_to_develop_a_secure_OS_for_industrial_control

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@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

46. *October 18, County 10* – (Wyoming) **Strong winds knock down a Wyoming.com tower in eastern Fremont County.** The October 16 wind storm that blew through Fremont County, Wyoming, knocked out one of Wyoming.com's service towers. The company's vice president said the tower that fell was near Shoshoni and served the Town of Shoshoni and parts of the rural Missouri Valley area. Internet service to those customers was interrupted by the fall. The director of Sales, Marketing, and Public Policy said a return of service date to affected customers has not yet been determined. He added that the company had to essentially rebuild the tower.
    Source: http://county10.com/2012/10/18/strong-winds-knock-down-a-wyoming-com-tower-in-eastern-fremont-county/

For another story, see item **32**

[Return to top]

Commercial Facilities Sector

47. *October 19, WRC 4 Washington D.C.* – (Virginia) **Man charged in Molotov cocktail-type incident in Ballston mall.** Police charged a suspect who was arrested October 18 after a Molotov cocktail-type device was tossed from the third floor of the Ballston Common Mall in Arlington, Virginia. The suspect was charged in Arlington County with reckless endangerment, attempted malicious bodily injury by use of fire, and use of a fire bomb. He was also charged with arson, a federal charge. He was due to appear in Arlington County Court October 19 for a preliminary hearing. He was also scheduled to appear in federal court in Alexandria October 19. Police said he dropped a 40-ounce beer bottle with a lit wick down into the basement-level food court of the mall. The bottle shattered but did not ignite. Authorities found three similar bottles in a bag on the third floor. The suspect was taken into custody about 3 hours later near the Court House Metro station. He was interviewed by local and federal authorities, including the joint terrorism task force. The food court shut down following the incident, but mall customers were not required to leave. However, the mall did not let in any new shoppers until over 5 hours after the incident. Wilson Boulevard eastbound was shut down for several hours during the investigation.

Source: http://www.nbcwashington.com/news/local/Man-Charged-in-Molotov-Cocktail-Type-Incident-in-Ballston-Mall-174945451.html

48. *October 19, KJRH 2 Tulsa* – (Oklahoma) **Murder suspect in standoff at hotel dead of self-inflicted wound.** The suspect in an October 18 Tulsa, Oklahoma homicide was dead after an hours-long standoff with police at a hotel, KJRH 2 Tulsa reported October 19. Officials said the suspect died of a self-inflicted wound. Tulsa police and the Special Operations Team evacuated part of a Days Inn October 19. They believed the suspect who killed his ex-wife's boyfriend was staying in one of the rooms. Officers surrounded the hotel room and began evacuating some guests. Hours after police made contact with the suspect, shots were heard across the street from the Days Inn. A Tulsa Police Department spokesman told a reporter the gun shots were from inside the room and were not directed at police. The police were unable to make contact with the suspect after the shots were fired. Later the suspect was confirmed dead from a self-inflicted wound. Police quickly to identified him as the suspect in the deadly shooting October 18.
Source: http://www.kjrh.com/dpp/news/local_news/police-in-hotel-standoff-with-murder-suspect

[Return to top]

National Monuments and Icons Sector

49. *October 19, Duluth News-Tribune* – (Minnesota) **Four months after being devastated by floods, popular Northland State park to reopen Monday.** Jay Cooke State Park in Minnesota was set to reopen October 22, 4 months after flooding washed away roads, trails, and bridges, Duluth News Tribune reported October 19. Park visitors, however, were restricted to driving into the park from the west, and only as far as park headquarters and the campground. Minnesota Highway 210 was expected to be fully reopened to the public by 2013 or 2014. By October 22, the park would reopen its office, interpretive center, campground, and camper cabins to the public. The June flooding washed out a 9-foot-diameter overflow pipe near the Thomson Bridge, and caused washouts and landslides along Highway 210, which is built on hills of unstable clay and silt in the park. The biggest problem was between park headquarters and Oldenburg Point, where floodwaters tore a 50-foot-deep, 250-foot-wide gap through the highway after an earthen embankment on Forbay Lake, a part of Minnesota Power's reservoir/power generation system, gave way. Minnesota Department of Transportation engineers and consultants were working to develop a solution for reopening the road. Minnesota Power was working with the Federal Energy Regulatory Commission planning the restoration of Forbay Lake.
Source: http://www.duluthnewstribune.com/event/article/id/247015/group/homepage/

[Return to top]

Dams Sector

50. *October 19, Associated Press* – (Louisiana) **8M contract awarded to protect Plaquemines pumps.** The U.S. Army Corps of Engineers said October 18 it had awarded an $8.1 million contract to Aquaterra-CAYO to build a floodwall to protect the Diamond Pump Station in Plaquemines Parish, Louisiana, from surge. The Corps began issuing contracts to give southern parts of Plaquemines better hurricane protection. Aquaterra-CAYO will build a concrete T-wall in front of the pump station and discharge pipes through the floodwall. The Corps have started work on upgrading 37 miles of back levees and completing other flood protection work in the parish. Back levees in Plaquemines were overtopped by surge during Hurricane Isaac at the end of August, causing widespread flooding.
Source: http://www.timesunion.com/news/article/8M-contract-awarded-to-protect-Plaquemines-pumps-3963493.php

51. *October 19, Pittsburgh Tribune-Review* – (Pennsylvania) **Earthen dams require watchful eye in Pennsylvania.** Workers moved huge amounts of dirt and poured concrete for part of the Oneida Dam and Reservoir in Oakland, Butler County, Pennsylvania for the dam’s new spillway, the Pittsburgh Tribune-Review reported October 19. Contractors were expanding the spillway with a layer of roller-compacted concrete on the 94-year-old dam, replacing its dirt face. Once work is done, expected in 2013, the chance of a breach during a heavy rain or flood will be practically none, officials said. There are 2,272 earthen dams in Pennsylvania. Of those, 1,030 need some type of repair, officials with the Pennsylvania Department of Environmental Protection (DEP) said. Needed repairs span from reversing erosion to expanding spillway capacity to clearing trees growing on the dam. No dam is in imminent danger of collapse, officials said. Still, when a major storm hits, State and local officials keep an eye on about 100 dams across Pennsylvania, most of them earthen. Some may be aging or deteriorated. Others may be fragile because they are in the midst of repairs. The DEP would not release the dams’ locations, citing security concerns.
Source: http://triblive.com/news/allegheny/2785517-74/dam-dams-county-officials-oneida-dep-state-butler-earthen-pennsylvania#axzz29kdlSBlY

52. *October 19, Homeland Security News Wire* – (National) **Corps: Absolute flood protection along Missouri River is impossible.** A U.S. Army Corps of Engineers report said that absolute flood protection along the Missouri River is impossible, so the basin needs to prepare and plan for flooding in the future, Homeland Security News Wire reported October 19. “All of us bear a shared responsibility for reducing flood risk,” the report said. The Corps said it bears responsibility for the Missouri River flood in 2011, and acknowledged that it is now responsible for implementing lessons learned from the flood. Victims and political leaders declared that a disaster like that should never happen again. The Corps, however, said it cannot guarantee that floods of such magnitude can be prevented. The report said that the system of dams, reservoirs, and levees generally functioned as designed and their management prevented nearly $8.2 billion in damage. Still, a number of improvements must be made to reduce the likelihood and consequences of future floods. The Corps said it was on track to make improvements to weather forecasting, communications, collaborations, and additional

changes to make sure the system is maintained and operated.
Source: http://www.homelandsecuritynewswire.com/dr20121019-corps-absolute-flood-protection-along-the-missouri-river-is-impossible

53. *October 18, Milwaukee-Wisconsin Journal Sentinel* – (Wisconsin) **DNR gives extension for Estabrook Dam improvements.** The Wisconsin Department of Natural Resources (DNR) agreed to extend the deadline for Milwaukee County to make repairs to the Estabrook Dam on the Milwaukee River to December 31, 2014, the Milwaukee-Wisconsin Journal Sentinel reported October 18. The county is under orders from the DNR to fix or tear down the aging dam. A wastewater management engineer with the DNR said that the agency has verbally agreed to a request by the county for more time. A county executive's 2013 budget included $4.2 million for removal of polluted sediment and improvements at the dam. Due to the current structural problems, the DNR ordered that the gates of the dam must stay open, keeping water levels down.
Source: http://www.jsonline.com/news/milwaukee/dnr-gives-extension-for-estabrook-dam-improvements-8579au3-174838161.html

54. *October 18, Fort Myers News-Press* – (Florida) **Army Corps of Engineers slowing Lake Okeechobee releases.** The U.S. Army Corps of Engineers is slowing ecologically damaging fresh water releases from Lake Okeechobee to the Caloosahatchee River in Florida, the Fort Myers News-Press reported October 18. Flows were as high as 8,000 cubic feet per second at the W.P. Franklin Lock water control structure in recent weeks. The new Corps release plan said that flow will drop to 3,000 cubic feet per second. The Caloosahatchee was one of two river systems used to drain Lake Okeechobee when water levels reach 16 feet or so above sea level. The Caloosahatchee was not connected to Lake Okeechobee historically, and too much fresh water from the lake can wash out the brackish estuary conditions needed to sustain various marine life, birds, and sea grasses. Serious environmental harm to the estuary can occur when lake releases reach 4,500 cubic feet per second or more of flow at the Franklin Lock.
Source: http://www.news-press.com/article/20121018/GREEN/121018014/Army-Corps-Engineers-slowing-Lake-Okeechobee-releases?odyssey=tab|topnews|text|Home

[Return to top]

NTAS
National Terrorism Advisory System
NO ACTIVE ALERTS
www.DHS.gov/alerts

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 ten 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)387-2273
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.