



Homeland
Security

Daily Open Source Infrastructure Report

14 November 2012

Top Stories

- People living in 31 homes within a half-mile radius of a train derailment site in Louisville, Kentucky, were again forced from their homes November 13 while dangerous chemicals were removed from the scene. – *Louisville Courier Journal* (See item [4](#))
- November 12, Lockheed Martin cited a dramatic growth in the number and sophistication of international cyberattacks on its networks and said it was contacting suppliers to help them bolster their security. Company officials also said about 20 percent of the threats directed at Lockheed networks were considered prolonged and targeted attacks by a nation state or other group trying to steal data or harm operations. – *Reuters* (See item [8](#))
- U.S. Food and Drug Administration inspectors released a 20-page report on Ameridose LLC November 12, claiming the Massachusetts drug company that has supplied dozens of Tennessee health-care facilities failed to properly test for the sterility of its products and did not investigate multiple complaints, including one case categorized as life-threatening. – *Nashville Tennessean* (See item [28](#))
- Two Digital Bond posts the week of November 5 showcase researcher findings on how easy it is to find industrial control systems (ICS) that have already been compromised, and that just fixing Supervisory control and data acquisition (SCADA) vulnerabilities is an ongoing process, not a solution. – *Infosecurity* (See item [42](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
 - [National Monuments and Icons](#)
-

Energy Sector

1. *November 13, Associated Press* – (Idaho) **Thieves steal \$25K in copper wire from site.** A construction company said thieves stole more than \$25,000 in copper wire from an Elmore County, Idaho construction site. Western Construction employees discovered the industrial cable used to run heavy equipment was missing November 12 from the site near Interstate 84. Western Construction estimated replacing the wire and repairing damage to equipment will cost \$50,000. The company is offering a \$5,000 reward for information that leads to an arrest.
Source: <http://www.newstimes.com/news/crime/article/Thieves-steal-25K-in-copper-wire-from-site-4032608.php>

2. *November 13, CNN* – (New Jersey; New York) **Costs from Sandy into the billions as thousands struggle, still, without power.** The outward signs of recovery were everywhere November 12 across the Northeast nearly 2 weeks after Superstorm Sandy struck: Power restored to tens of thousands, bridges and tunnels reopened, and limited train and ferry service was up and running. Gas rationing continued in New York City and Long Island’s Nassau and Suffolk counties. The New Jersey governor said it would take time to restore necessary services for those who live on New Jersey’s barrier islands because so much infrastructure was destroyed. Not long after the superstorm, more than 8.6 million people were without power, the U.S. Department of Energy said. As of November 11, that was down to about 160,000 customers. Long Island Power Association said November 12 it restored service to more than 97 percent of customers whose homes and business can safely receive power. Over 10,000 linemen and tree trim crews remained at work for those still in the dark. Con Edison announced its last New York City customers affected got their power back, while all Westchester County customers had electricity back by November 12.
Source: <http://www.cnn.com/2012/11/12/us/northeast-weather/index.html>

3. *November 8, Wall Street Journal* – (International) **Stuxnet infected Chevron's IT network.** Stuxnet infected Chevron's network in 2010, shortly after it escaped from its intended target, the Wall Street Journal reported November 13. Chevron found Stuxnet in its systems after the malware was first reported in July 2010, said the general manager of the earth sciences department at Chevron. Chevron was not adversely affected by Stuxnet, said a Chevron spokesman. Chevron's experience with Stuxnet appears to be the result of the unintentional (and perhaps, inevitable) release of malware upon a larger network, much like an experimental virus escaping from a medical lab. Chevron is the first U.S. company to acknowledge that its systems were infected by Stuxnet, although most security experts believe the vast majority of hacking incidents go unreported for reasons of security or to avoid embarrassment. The devices used in industrial equipment and targeted by Stuxnet are made by huge companies, including Siemens.
Source: <http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/>

For another story, see item [42](#)

[\[Return to top\]](#)

Chemical Industry Sector

4. *November 12, Louisville Courier Journal* – (Kentucky) **Latest evacuation for train derailment to begin Tuesday and could last up to four days.** Residents around the site of the derailment of 13 Paducah & Louisville Railway (P&L) cars were again forced from their homes November 13 while dangerous chemicals were removed from the scene, reported the Louisville Courier-Journal. People living in 31 homes within a half-mile radius of the derailment were asked to evacuate, the Louisville Metro Emergency Management Agency said November 12. P&L said the evacuation order will be in place until all the chemicals are taken away, which could take three or four days. Dixie Highway from Kentucky 44 to the Salt River bridge will also be closed starting November 13 and will stay closed for the duration of the clean up. A no-fly-zone will be in effect a half mile around the site and Ohio River traffic in the area will be stopped while tens of thousands of gallons of highly toxic hydrogen fluoride and flammable butadiene are offloaded from derailed tank cars.
Source: <http://www.courier-journal.com/article/20121112/NEWS01/311120029/Tuesday-evacuation-order-last-long-four-days-residents-living-around-derailment-site?odyssey=nav/head>
5. *November 9, Milwaukee-Wisconsin Journal Sentinel* – (Wisconsin) **Tab for chemical cleanup in Slinger reaches \$135,000.** Emergency removal of nearly 9,000 gallons of hazardous chemicals from an abandoned metal plating factory in Slinger, Wisconsin, cost about \$135,000, a U.S. Environmental Protection Agency (EPA) official said November 9. Federal contractors took out more than 315 barrels, drums, vats, and large jugs containing chemicals and metal plating wastes from Niphos Coatings. Federal contractors in September inventoried 8,868 gallons of hazardous chemicals stored in containers of all sizes. Two of the chemicals left behind in the building - nitric acid and sodium cyanide - are considered extremely hazardous. Now that the cleanup is

completed, an office of the EPA will determine if the business owner is able to reimburse the agency - and taxpayers - for any portion of the \$135,000 bill, an EPA coordinator said.

Source: <http://www.jsonline.com/news/ozwash/tab-for-chemical-cleanup-in-slinger-reaches-135000-437ijqu-178150591.html>

For another story, see item [30](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials and Waste Sector

6. *November 13, Lacey Patch* – (New Jersey) **NRC inspecting Oyster Creek response to Sandy.** The Nuclear Regulatory Commission (NRC) began an inspection November 13 of the Oyster Creek Generating Station in Lacey, New Jersey, in response to issues related to Hurricane Sandy. Three inspectors are reviewing activities related to water level increases at the plant’s water intake structure during the storm and will expand on reviews made during and after the storm by the NRC’s resident inspectors assigned to Oyster Creek. “Because the reactor was out of service at the time of the storm for a previously scheduled refueling and maintenance outage, plant operators did not have to contend with the possibility of a reactor shutdown as Sandy passed through the area. There were no immediate safety concerns,” the NRC Region I Administrator said. “Nevertheless, there are certain observations involving procedures and on-site activities that surfaced during the event warranting a closer look. This Special Inspection will focus on those areas to gain a better understanding of how the intake water level information was monitored and communicated during the event.”

Source: <http://lacey.patch.com/articles/nrc-inspecting-oyster-creek-response-to-sandy>

7. *November 11, Associated Press* – (New York) **Fire triggers shutdown at upstate NY nuke plant.** The FitzPatrick nuclear power plant in Scriba, New York, was shut down for the second time in a week November 11 due to a fire in the plant’s main transformer. Plant owner Entergy Nuclear said the fire was extinguished in about 1 hour. The company said there was no release of radiation and no danger to employees or the public. It was reported as an “unusual event,” the lowest of four event classifications by the Nuclear Regulatory Commission.

Source: <http://www.newsday.com/news/region-state/fire-triggers-shutdown-at-upstate-ny-nuke-plant-1.4211439>

[\[Return to top\]](#)

Critical Manufacturing Sector

Nothing to report

[\[Return to top\]](#)

Defense Industrial Base Sector

8. *November 12, Reuters* – (International) **Lockheed says cyber attacks up sharply, suppliers targeted.** November 12, the U.S. Department of Defense’s number-one supplier, Lockheed Martin, cited dramatic growth in the number and sophistication of international cyberattacks on its networks and said it was contacting suppliers to help them bolster their security. The company’s vice president and chief information security officer said about 20 percent of the threats directed at Lockheed networks were considered “advanced persistent threats,” prolonged and targeted attacks by a nation state or other group trying to steal data or harm operations. She said the company had seen “very successful” attacks against a number of the its suppliers, and was focusing heavily on helping those companies improve their security.
Source: <http://www.reuters.com/article/2012/11/13/net-us-lockheed-cyber-idUSBRE8AC02S20121113>

[\[Return to top\]](#)

Banking and Finance Sector

9. *November 13, Softpedia* – (International) **Experts investigate malware used in Gozi-Prinimalka campaign against US banks.** In October, RSA revealed that cybercriminals were planning to launch massive trojan attacks against several U.K. banks. Now, Trend Micro researchers analyzed a few samples of the malware that will likely be utilized in the Gozi-Prinimalka campaign, Softpedia reported November 13. One of the samples, BKDR_URSNIF.B, is designed to monitor its victims’ browsing activities and collect any information elated to financial institutions such as Wells Fargo, PayPal, and Wachovia. Another sample, BKDR_URSNIF.DN, starts by searching for a specific Firefox registry entry. If this entry is found, a file that drops JS_URSNIF.DJ is created. If the registry is not located, the malware does not steal any information, but it still performs other malicious tasks. JS_URSNIF.DJ is the JavaScript that is actually responsible for stealing information. It injects itself into specific Web sites and waits for the victims to enter their credentials. Once the information is harvested, it sends it back to its master via HTTP POST requests. According to the researchers, several command and control servers are utilized by these pieces of malware. Experts also managed to retrieve the names of three additional targets by analyzing the malware’s configurations files. TDBank, Firstrade Securities, and optionsXpress are on the list of targets. All of the institutions have been notified.
Source: <http://news.softpedia.com/news/Experts-Investigate-Malware-Used-in-Gozi-Prinimalka-Campaign-Against-US-Banks-306535.shtml>
10. *November 12, Des Plaines Patch* – (Kentucky; Illinois) **Police: ‘Elmer Fudd Bandit’ arrested.** Law enforcement reported they arrested a man who is suspected in four armed bank robberies in the Chicago area, an attempted armed bank robbery in Des Plaines, Illinois, and a bank robbery in Louisville, Kentucky, the Des Plaines Patch reported November 12. The man, dubbed the “Elmer Fudd Bandit” by the FBI due to the flannel shirts and caps seen in surveillance video, was arrested at an apartment building by Kentucky State Police and the Grayson County Sheriff’s Department. Law enforcement received an anonymous tip following a bank robbery that occurred at a U.S. Bank in Louisville November 8, the Grayson County News Gazette reported. In

addition to the similar clothing worn by the male subject in surveillance video, in many of the incidents the man approached a bank teller with a notepad that stated to give him money, and he threatened to injure the teller.

Source: <http://desplaines.patch.com/articles/police-elmer-fudd-bandit-arrested>

11. *November 12, Business Technology News* – (International) **PayGate confirms security breach.** The South African online payment service provider PayGate confirmed its systems were breached in August and some credit card numbers may have been exposed, BusinessTech reported November 12. It follows an admission November 9 by the Payments Association of South Africa that private credit card and banking details were leaked during a breach at a company which processes online transactions. “We detected unauthorised activity on our servers in August and immediately took action to secure our systems and protect our customers,” said PayGate’s managing director. He said that while some credit card details may have been exposed, “the card associations and banks are pro-actively monitoring all credit cards processed during this period and will contact cardholders directly if necessary.” He stressed that PayGate did not store any personal details like addresses or ID numbers, although it does store email addresses.

Source: <http://businesstech.co.za/news/general/26305/paygate-confirms-security-breach/>

12. *November 12, Associated Press* – (New York; National) **NY gets \$9.5M from NC firm over soldier debt fraud.** The New York Attorney General reached a \$9.5 million settlement with retailer SmartBuy and its affiliated companies over debt fraud aimed at soldiers, the Associated Press reported November 12. The Attorney General said SmartBuy operated from a kiosk and small storefront at Salmon Run Mall near the Fort Drum Army post and ruined the credit of thousands of soldiers through fraudulent charges. The settlement, along with an earlier one with SmartBuy, wipes out \$12.9 million in debt for more than 4,000 soldiers nationwide. The Attorney General said SmartBuy salespeople talked soldiers into payment contracts with hidden fees and exorbitant interest. Fayetteville, North Carolina-based SmartBuy closed its local operations after the Attorney General demanded it stop deceptive practices and reimburse soldiers. Investigators found that SmartBuy purchased merchandise, marked it up 200-325 percent, and added interest of 10-25 percent. It locked soldiers into credit agreements with undisclosed fees and high interest, paid directly from military paychecks. The settling entities include Frisco Marketing of New York, doing business as SmartBuy and SmartBuy Computers and Electronics; Integrity Financial of North Carolina; Britlee and GJS Management; all owned and/or operated by a North Carolina family. The settling companies will contractually release all of the approximately 358 New York soldiers, and an additional 3,963 soldiers nationwide from their debt. They will also clear all negative credit reports related to the contracts and will pay a \$150,000 penalty to New York. Under a consent order and judgment, the companies are banned permanently from doing business in New York.

Source:

http://seattletimes.com/html/nationworld/2019667168_apusmilitaryconsumersfraud.html

[\[Return to top\]](#)

Transportation Sector

13. *November 13, WPVI 6 Philadelphia* – (New Jersey) **School bus involved in GSP crash failed inspection.** The bus involved in a November 12 crash on the Garden State Parkway failed an inspection in October, reported WPVI 6 Philadelphia. The crash happened in Egg Harbor Township, New Jersey, where students were heading home from Atlantic City to their Somers Point campus. Twenty-two students were taken to a local hospital where many were released November 12. Several others were taken to a medical center. This same bus failed an inspection in October, in part because the tires were in bad condition. The bus was then re-examined and passed the inspection. The right lane of the northbound Garden State Parkway was closed for approximately 2 hours.

Source: <http://abclocal.go.com/wpvi/story?section=news/local&id=8883526>

14. *November 12, Wall Street Journal* – (New Jersey; New York) **PATH trains running again from N.J. to Manhattan.** The Port Authority of New York and New Jersey said November 12 that limited service has been restored to its Port Authority Transit Hub (PATH) commuter trains running between New Jersey and New York City. PATH trains were operating on a limited schedule, seven days a week, from Newark to 33rd Street in Manhattan after being knocked out late October by flooding from Hurricane Sandy.

Source: http://articles.marketwatch.com/2012-11-12/general/35060141_1_journal-square-path-trains-newark-penn-station

For another story, see item [4](#)

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report

[\[Return to top\]](#)

Agriculture and Food Sector

15. *November 12, U.S. Food and Drug Administration* – (National) **Voluntary product recall for Jimmy Dean French Toast & Sausage Sandwich for undeclared allergens.** Jimmy Dean voluntarily recalled a partial production run of its French Toast & Sausage Sandwich with the code 12292P1 on the back label November 10 because the product may contain the undeclared allergens egg and soy, reported the U.S. Food and Drug Administration. This recall is due to a labeling error, in which the wrong ingredient statement may have been applied to a small number of sandwiches. The recall affects 1,110-pounds of product distributed to 10 States.

Source: <http://www.fda.gov/Safety/Recalls/ucm327724.htm>

16. *November 10, U.S. Food and Drug Administration* – (National) **Spence & Co issues a voluntary recall of 4 oz New York Style Nova Lox lot number 9720704 because of possible health risk.** Spence & Co Ltd, of Brockton, Massachusetts, voluntarily recalled its New York Style Nova Lox, 4-ounce, Code/Lot: 9720704, November 9 because of possible contamination by *Listeria monocytogenes*. The recall affects a total of 1,563 packs of product. The recalled product was sent to distributors in Illinois, Missouri, New Jersey, Massachusetts, and in the Detroit area. It was also distributed to retail stores in 16 States including: Earthfare, Shaws Supermarkets, Roche Bros, and Fresh Markets. Two possible product related illnesses were reported; the bacterium was discovered during routine sampling.
Source: <http://www.fda.gov/Safety/Recalls/ucm327715.htm>
17. *November 10, U.S. Food and Drug Administration* – (National) **Frito-Lay issues voluntary recall of Grandma’s Peanut Butter Sandwich Creme Cookies and Grandma’s Peanut Butter Mini Sandwich Creme Cookies due to undeclared milk and egg.** Frito-Lay announced November 9 the nationwide voluntary recall of Grandma’s Peanut Butter Sandwich Crème cookies and Grandma’s Peanut Butter Mini Sandwich Crème cookies because they contain undeclared milk and egg, reported the U.S. Food and Drug Administration. The products are sold in retail stores nationwide. The affected packages are 3.025-ounce packages of the Peanut Butter Sandwich Crème cookies with a sell by date of March 12, 2013 or earlier, and the 1.71-ounce Peanut Butter Mini Sandwich Crème cookies with a sell by date of May 21, 2013 or earlier.
Source: <http://www.fda.gov/Safety/Recalls/ucm327711.htm>
18. *November 9, U.S. Department of Agriculture Food Safety and Inspection Service* – (Wisconsin; Illinois) **Wisconsin firm recalls beef tongues that may contain specified risk materials.** Black Earth Meat Market Inc., a Black Earth, Wisconsin company, recalled approximately 99-pounds of beef tongue products November 9 because they may not have had the tonsils completely removed. The recalled products come in various size cases labeled as Black Earth Meats Natural Beef Tongues and Black Earth Meats Local Beef Tongues. The products were distributed to a restaurant in Wisconsin and a distributor in Illinois. The problem was discovered during a routine assessment at the establishment.
Source:
http://www.fsis.usda.gov/News_&_Events/Recall_073_2012_Release/index.asp

[\[Return to top\]](#)

Water Sector

19. *November 13, Associated Press* – (National) **Plan could halt river traffic.** The governor of Missouri and the barge industry implored the federal government to take steps to keep enough water flowing on the drought-ridden Missouri and Mississippi rivers to avert a potential “economic disaster.” Current corps plans would reduce the amount of water released from the Missouri’s upstream reservoirs starting the week of November 19. The corps said the week of November 5 that the flow reduction to minimum winter levels was the first of several conservation measures necessary if

drought conditions continue into 2013. The agency said precipitation levels remain below normal over the entire Missouri River basin. To compensate, many barge owners now are required to carry lighter loads, costing them more per ton to move cargo and requiring crews to dredge silt and other sediments from the river to clear passages. The American Waterway Operators said barges on those corridors carry 20 percent of the country's coal and more than 60 percent of its grain exports. A mix of other cargo — everything from petroleum products to lumber, sand, industrial chemicals, and fertilizer — also gets shipped by river.

Source: http://thesouthern.com/news/local/plan-could-halt-river-traffic/article_85f97e46-2d55-11e2-8656-0019bb2963f4.html

20. *November 12, Associated Press* – (Pennsylvania) **Pollution persists in Allegheny River in Western Pennsylvania.** Recent research shows high levels of an ultra-salty compound that could be linked to oil and gas drilling persist in the Allegheny River's Pittsburgh, Pennsylvania-area watershed, while the levels declined in the nearby Monongahela River, the Associated Press reported November 12. Bromide levels soared during a surge of Marcellus Shale gas drilling in 2009 and 2010. Although not considered a pollutant by themselves, the bromides combine with chlorine used in water treatment to produce compounds that can threaten public health. A recent Pittsburgh Water and Sewer Authority report found that high levels of bromides in the Allegheny just downstream from industrial brine treatment plants. The report also noted that bromide levels rose in rivers below where some coal-fired power plants discharge wastewater, which can also include bromides. A spokesman for the Pennsylvania Independent Oil and Gas Association said that State regulators do not set a limit on bromide discharges, and that the amount of wastewater that comes from conventional wells was decreasing. He also noted that the Water and Sewer Authority testing only identified elevated bromide levels in the Allegheny for part of the year, during periods of low river flow.

Source:

http://www.syracuse.com/news/index.ssf/2012/11/pollution_persists_in_alleghe.html

21. *November 12, Boston Herald* – (Massachusetts) **Worcester water supply crippled by broken main.** Water was in short supply throughout the Worcester, Massachusetts area for a while due to a water main break, but repair plans were slated for November 13, Worcester Department of Public Works and Parks Water Operations officials said November 12. There could be ongoing problems with low pressure and discoloration, city officials said, and, when the water returns, residents were urged to boil the water from their pipes before consuming it. The break occurred in a 30-inch water main November 12. "The break will cause disruption of the water supply to the entire city of Worcester, the Elm Hill Water District and Woodland Water District in Auburn, the town of Paxton, Century Drive corporate park in West Boylston, the Millbury Industrial Park, and possibly the town of Holden," Worcester officials said in a statement. Only after the regional water system is re-pressurized will samples be collected throughout the city to assure the water is safe to drink, a spokesman said. That may take two to four days after restoration of the water system to complete.

Source:

http://www.bostonherald.com/news/regional/view/20221112worchester_water_supply_crippled_by_broken_main/srvc=home&position=recent

22. *November 12, Homeland Security News Wire* – (National) **Cleanup of most contaminated U.S. groundwater sites unlikely for many decades.** At least 126,000 sites across the United States have contaminated groundwater that requires remediation, and about 10 percent of these sites are considered “complex,” meaning restoration is unlikely to be achieved in the next 50 to 100 years due to technological limitations, said a new report from the National Research Council reported on by the Homeland Security News Wire November 12. The report adds that the estimated cost of complete cleanup at these sites ranges from \$110 billion to \$127 billion, but that both the number of sites and costs are likely underestimates.
Source: <http://www.homelandsecuritynewswire.com/dr20121112-cleanup-of-most-contaminated-u-s-groundwater-sites-unlikely-for-many-decades>
23. *November 11, Long Island Newsday* – (New York) **Millions of gallons of partially treated sewage flowing into waterway.** Sixty-five million gallons of partially treated sewage from a plant that serves almost 40 percent of New York’s Nassau County residents are flushing each day into a waterway north of Long Beach — a result of damage from superstorm Sandy that could have far-reaching environmental implications, the Long Island Newsday reported November 11. Initial estimates from Nassau County said the sewage flow from the Bay Park Sewage Treatment Plant into Reynolds Channel could go on through about November 30 as workers try to fix the plant. A Department of Public Works spokesman said it is “undetermined” when the East Rockaway plant can resume fully treating sewage. The treatment pumps failed when the plant was flooded by a 9-foot wall of water pushed ashore by Sandy. The daily volume amounts to 1.95 billion gallons of sewer water a month that has been cleared of solids and chlorinated, but not fully treated, pouring into the channel, which flows into Rockaway Inlet and the Atlantic Ocean. It could be 6 to 12 months before the facility is fully repaired, according to a statement from the office of the Nassau County Executive.
Source: <http://www.newsday.com/long-island/millions-of-gallons-of-partially-treated-sewage-flowing-into-waterway-1.4212211>
24. *November 9, Associated Press* – (Maryland) **Wicomico Co. residents face tainted groundwater.** Maryland environmental officials warned Wicomico County residents that an industrial solvent has likely been in their water supply for at least several years. The Daily Times of Salisbury reported that the State Department of the Environment briefed residents on the contamination at a November 8 meeting. Officials said they were not sure who was responsible for the trichloroethene contamination, but that the chemical was likely dumped from gallons or drums. The colorless liquid is often used to remove grease from metal. The county health department says 46 of the 113 wells that were tested are above the threshold for trichloroethene.
Source: <http://www.wtop.com/46/3112665/Wicomico-Co-residents-face-tainted-groundwater>

25. *November 8, Associated Press* – (Alaska) **Remote Alaska village monitoring water, fearing supply won't last through winter.** Residents of a small Alaska Native village facing a severe water shortage are monitoring their water usage as they struggle to stretch their reserves as far into winter as possible, with help coming from as far away as Minnesota, the Associated Press reported November 8. "It's very, very clear that we won't have enough," the Kivalina city administrator said. Kivalina has two big storage tanks that hold a total of about 1.2 million gallons of water. When full, it is a six-month water supply for the community's 400 residents. However, Kivalina has only July and August to fill the tanks before the pipeline freezes or the river gets too icy. This year, the village was ready to fill the tanks but lacked the necessary funds for labor and the fuel to run the water transferring system. Then the heavy August storms, which flooded Kivalina's landfill and broke the pipe in places, left the village school without clean water and postponing the start of classes for five weeks. In September, the Alaska governor declared a disaster because of the storms, making State funds available for pipeline repairs.

Source: <http://www.foxnews.com/us/2012/11/08/remote-alaska-village-monitoring-water-fearing-supply-wont-last-through-winter/>

[\[Return to top\]](#)

Public Health and Healthcare Sector

26. *November 13, Associated Press* – (Minnesota) **Minnesota reports 12th fungal meningitis case.** Minnesota reported its 12th confirmed case of fungal meningitis in a national outbreak linked to tainted steroids from a Massachusetts pharmacy, the Associated Press reported November 13. The assistant State epidemiologist said the new case is a Twin Cities area man who received an injection at a metro clinic. He said he had some symptoms earlier but got better. However, in the last few weeks, his symptoms including headaches got worse again.

Source: http://www.necn.com/11/13/12/Minnesota-reports-12th-fungal-meningitis/landing_health.html?&apID=d14e802b73a748b49ff0303dd75d3e7d

27. *November 12, Associated Press* – (New York) **Sandy-damaged NY hospitals to be closed for weeks.** An official said New York City's storm-damaged Bellevue and Coney Island hospitals will not be fully running until early 2013, the Associated Press reported November 12. Both hospitals were evacuated after being inundated by Superstorm Sandy. Coney Island is already running outpatient services. The City Health and Hospitals Corp. president said November 12 that Bellevue expects to start offering outpatient services November 19. He said the operating rooms, critical care units, and other facilities could open by January 1, 2013 at Coney Island and the first week of February 2013 at Bellevue.

Source: <http://www.stamfordadvocate.com/news/article/Sandy-damaged-NY-hospitals-to-be-closed-for-weeks-4030293.php>

28. *November 12, Nashville Tennessean* – (Massachusetts) **Meningitis outbreak: Inspectors find bird flying through Ameridose pharmacy.** U.S. Food and Drug Administration (FDA) inspectors found a Massachusetts drug company that has

supplied dozens of Tennessee health-care facilities failed to properly test for the sterility of its products and did not investigate multiple complaints, including one case categorized as life-threatening. The 20-page report on Ameridose LLC issued November 12 listed multiple violations of federal regulations. Inspectors even reported seeing a bird flying through a storage area for sterile drugs. Ameridose, based in Westborough, Massachusetts, has the same owners as the New England Compounding Center, which has been blamed for a nationwide outbreak of fungal meningitis that has killed 31 patients, including 13 in Tennessee. A spokesman for the company said Ameridose was preparing a full response to the FDA report.

Source: <http://www.wbir.com/news/article/241721/2/Meningitis-outbreak-Inspectors-find-bird-flying-through-Ameridose-pharmacy>

29. *November 12, Macon Telegraph* – (New Hampshire; National) **Houston Healthcare notifies additional 400 patients of hepatitis C investigation.** About 4 months after a former Houston Healthcare contract employee was accused of spreading hepatitis C to patients in a New Hampshire hospital, local officials have alerted hundreds of additional Houston Medical Center patients who were treated while he worked there, the Macon Telegraph reported November 12. Houston Healthcare recently sent letters to more than 400 patients, suggesting they be tested for the life-threatening infection. The employee, who temporarily worked in Houston Medical Center’s heart catheterization lab, is accused of infecting more than 30 people, mainly in New Hampshire, and possibly infecting many more patients across the country with tainted syringes. While letters were sent this summer to fewer than 100 local patients who might have had contact with the employee, Houston Healthcare was encouraged to notify additional patients who were treated in an area where he worked. As part of a multi-State investigation, Houston Healthcare began alerting those additional patients in September, according to a statement from the hospital.
Source: <http://www.macon.com/2012/11/12/2247042/houston-healthcare-notifies-additional.html>
30. *November 10, Associated Press* – (Nebraska) **Chemical leak forces hospital evacuation.** A Fairbury, Nebraska hospital was reopened November 10 after being evacuated November 10 because of a chemical leak. Jefferson Community Health Center south of Lincoln was evacuated after a hazardous-materials unit discovered a chemical leak in the hospital’s laundry room. Assisted living and long-term care tenants were taken to a nearby church after the leak of the unidentified chemical. Four patients were taken to other health care facilities.
Source: <http://www.wowt.com/news/headlines/Chemical-Leak-Forces-Hospital-Evacuation-178456061.html>

[\[Return to top\]](#)

Government Facilities Sector

31. *November 12, WYMT 57 Hazard* – (Kentucky) **Letcher County courthouse damaged in earthquake.** A November 10 earthquake struck just eight miles from the city of Whitesburg, Kentucky. Damage from the 4.3 magnitude quake was light, but a few

homes and the county courthouse sustained some structural damage. Officials are still assessing the damage to the courthouse.

Source: <http://www.wkyt.com/wymt/home/headlines/Letcher-County-courthouse-damaged-in-earthquake-178984201.html>

32. *November 12, KUSA 9 Denver* – (Colorado) **Accidental shooting at University of Colorado dental school.** Two people suffered minor injuries November 9 when a gun accidentally went off at the University of Colorado School of Dental Medicine at the Anschutz Medical Campus in Aurora, Colorado. A spokesman for the university said the owner of the gun is a school employee and is currently on administrative leave. The injuries did not require hospitalization. A university spokesman said campus police were investigating the incident, and that the gun's owner had a concealed carry permit for it. The University of Colorado for many years enforced a ban on all weapons on its campuses, but in March 2012 the Colorado Supreme Court struck down the university's gun ban, which means visitors and staff members with a valid concealed carry permit are allowed to have guns on campus.

Source: <http://www.9news.com/news/local/article/299501/222/Accidental-shooting-at-CU-dental-school>

33. *November 12, WWBT 12 Richmond* – (Virginia) **Tuckahoe Elementary cancels Tues. and Weds. classes due to fire.** Henrico County, Virginia Public School officials decided to cancel classes at Tuckahoe Elementary School November 13 and November 14 after a weekend fire. An electrical fire November 11 triggered five fire trucks to rush to the scene. A fire captain said 75 percent of the school is covered in soot. Tuckahoe Elementary School closed November 12 for students. Henrico School officials said they cannot let students into the building with the huge amount of smoke damage left from a relatively small fire. The issue remaining is the toxic soot left by smoke. The closure will give staff time to ready Short Pump Middle School, where students will begin attending class November 15. Officials hope the move will only last a couple weeks, while Tuckahoe Elementary is restored to normal conditions.

Source: <http://www.nbc12.com/story/20068587/fire-cleanup-forces-tuckahoe-elementary-in-henrico-to-close>

For more stories, see items [12](#), [13](#), and [25](#)

[\[Return to top\]](#)

Emergency Services Sector

34. *November 12, KGO 7 San Francisco* – (California) **San Jose marine fatally shot by police officers.** Officers in Palm Springs, California, insisted they had no choice but to open fire on a 22-year-old marine November 10 in a parking garage. Police said he and his friend began yelling derogatory comments toward two officers on bike patrol at which point, the officers instructed him to turn off his car. Police said he refused, which prompted one of the officers to climb through his passenger side window. That was when the marine began stepping on the gas. "The suspect accelerated directly toward the second officer striking him, and continued on with the initial officer suspended

from the passenger side window,” the Palm Springs police chief said. Police said the officers feared for their lives and began shooting at the marine. He was pronounced dead shortly after. The officers were treated and released from the hospital.

Source: http://abclocal.go.com/kgostory?section=news/local/south_bay&id=8883377

35. *November 11, CNN* – (Michigan) **Man, 64, killed after opening fire inside Michigan police station.** A man walked into a Southfield, Michigan police station November 11 and opened fire, precipitating a shootout that ended with him dead and a police officer wounded, police said. The man entered the building that houses the Southfield Police Department with a handgun and pointed it at an officer sitting behind bullet-proof glass, said a police spokesman. Refusing requests to put down the gun, the man started firing at the desk officer. The first officer to respond was shot in the shoulder, the spokesman said. That officer and others returned fire, hitting the shooter. Both wounded men were treated at the scene and moved to a nearby hospital. The man later died from his injuries at the hospital. Authorities did not know why he opened fire at the police station. The wounded officer was in stable condition.
Source: http://news.blogs.cnn.com/2012/11/11/man-64-killed-after-opening-fire-inside-michigan-police-station/?hpt=ju_c2
36. *November 10, Associated Press* – (Mississippi) **Another inmate charged in deadly Miss. prison riot.** Another inmate was charged with participating in a deadly prison riot in Natchez, Mississippi, the Associated Press reported November 10. One guard was killed and 20 people were injured in the May 20 riot at the privately-run Adams County Correctional Facility, which holds illegal immigrants convicted of crimes in the U.S. The inmate was charged November 7. A complaint filed by an FBI agent said he assaulted a guard. He is at least the third inmate charged in the case.
Source: <http://www.wxvt.com/story/20060438/another-inmate-charged-in-deadly-miss-prison-riot>
37. *November 9, United Press International* – (Michigan) **Person enters Detroit police station with found grenade.** The Detroit Police Department’s Eastern District building was evacuated after a person walked in holding a grenade. The unnamed visitor entered the building November 9 and announced, “Look what I found,” a Detroit Police spokeswoman said. The incident prompted the closing of Gratiot Street, where the police office is located, the Detroit News reported. A bomb squad was called to the building and police public information officials said Department of Homeland Security personnel were assisting in the investigation.
Source: http://www.upi.com/Odd_News/2012/11/09/Person-enters-police-station-with-grenade/UPI-97561352492981/

[\[Return to top\]](#)

Information Technology Sector

38. *November 13, The Register* – (International) **Even a child can make a trojan to pillage Windows Phone 8.** A teenager crafted prototype malware for Windows Phone 8 just weeks after the official unveiling of the smartphone platform. The proof-of-

concept code is due to be demonstrated at the International Malware Conference (MalCon) in New Delhi, India, November 24. The teenager, who is a member of the Indian government-backed National Security Database program of information security professionals, created malware that attacked Microsoft's Xbox Kinect in 2011. Documents posted on the MalCon Web site ahead of the talk suggest he developed a trojan that poses as a legitimate application before stealing users' data, including contact numbers, text messages, and photos. Details are thin, so it is unclear whether the malware exploits a vulnerability in Windows Phone 8 or it simply tricks users into doing something daft, such as installing malicious code posing as a game or utility. Source: http://www.theregister.co.uk/2012/11/13/windows_phone_8_malware/

39. *November 12, Help Net Security* – (International) **One in four users at risk due to outdated browsers.** Nearly a quarter of users do not use the latest browser versions, and those using Mozilla Firefox are the slowest when it comes to updating, which leaves them open to Web-based attacks, Kaspersky Lab warns. Basing their results on the information collected from their 10 million randomly selected customers from different regions across the world, the company discovered that Chrome users are nearly as numerous as Internet Explorer (IE) ones (36.5 and 37.8 percent, respectively), while the numbers for Firefox (19.5 percent) keep falling. While the news is not good for Mozilla, it is for security, as only 69.5 percent of Firefox users use the latest two versions, but 94.7 percent of Chrome users and 96.5 percent of IE users do the same. Also, compared to Chrome users, Firefox users update to the newer version at a slower speed and more users tend to stay on the older version for a longer period of time. The research differentiates between older (but still supported) versions of the browsers and the outdated ones, but still point out that 23 percent of the users have not opted for the latest versions and the security improvement they bring. Source: <http://www.net-security.org/secworld.php?id=13934>
40. *November 12, Threatpost* – (International) **New Java attack introduced into Cool Exploit Kit.** A new exploit was found in the Cool Exploit Kit for a vulnerability in Java 7 Update 7 as well as older versions, a flaw patched by Oracle in Java 7 Update 9. Cool Exploit Kit was discovered in October and is largely responsible for dropping the Reveton ransomware. A new Metasploit module was introduced November 11 by a researcher, according to a frequent Metasploit contributor. He suggested it is likely the exploit has been in the wild for a period of time and has only now been integrated into an exploit kit. The new Java exploit, a sandbox escape, targets vulnerability CVE-2012-5076 that was repaired in Oracle's October 2012 Critical Patch Update. Attackers can run arbitrary code on compromised machines, the Metasploit contributor said. Source: http://threatpost.com/en_us/blogs/new-java-attack-introduced-cool-exploit-kit-111212
41. *November 12, The H* – (International) **Ruby update fixes hash flooding vulnerability.** The Ruby developers released an update to the 1.9.3 series of their open source programming language, fixing a denial-of-service (DoS) vulnerability. Ruby 1.9.3 patch level 327, labelled 1.9.3-p327, corrects a hash-flooding issue that could be exploited by an attacker to cause high CPU load that can result in a DoS. The problem can be caused by an error when parsing specially crafted sequences of strings. The

developers point out that the vulnerability is similar to another widespread DoS issue in hash algorithms that affected a number of programs including the 1.8.7 branch of Ruby. All Ruby 1.9.x versions prior to 1.9.3-p327, as well as all Ruby 2.0 pre-release versions prior to trunk revision 37575 including 2.0.0 preview 1 from earlier in November are affected. Users running these versions are advised to upgrade to the latest 1.9.3 patch level or trunk revision 37575 or later as soon as possible.

Source: <http://www.h-online.com/security/news/item/Ruby-update-fixes-hash-flooding-vulnerability-1748192.html>

42. *November 12, Infosecurity* – (International) **Researcher tracks down compromised ICS systems.** Supervisory control and data acquisition (SCADA) and industrial control systems' (ICS) security has been repeatedly questioned in recent months. Now, one researcher shows how easy it is to find ICS systems that have already been compromised, while another warns Siemens that just fixing SCADA vulnerabilities is an ongoing process, not a solution. In two Digital Bond posts the week of November 5, a researcher describes the SCADA vulnerability problem, and then a second researcher demonstrates how to locate such systems that have already been compromised. He concentrates on one particular system he found, "an extremely detailed DDS log." "First off," he writes, "this system has the SEL AcSELEerator Quickset and GE Enervista, so it was used to either review relay configurations or install relay configurations on SEL and GE digital protective relays." In other words, it effectively plugs into the national power grid. "This suggests a technician's laptop, one who works on a wide variety of electric power systems and other automation systems." However, the laptop was infected with two pieces of malware: The fake antivirus and backup program "Malware Protection Designed to Protect" and "Windows XP Recovery." Such malware is usually installed either by drive-by downloading or direct installation. Source: <http://www.infosecurity-magazine.com/view/29267/researcher-tracks-down-compromised-ics-stems/>

43. *November 10, The H* – (International) **Worth reading: Dropbox is "quite secure"**. Security specialists from the IT department at EADS cast a critical eye on the Dropbox cloud storage service and recently presented their findings at the Hack.LU security conference. They explained the trickery used by the service's developers to encrypt the Python-based desktop client, showed how the client protects its configuration, and demonstrated how data is exchanged. The researchers said they found no major vulnerabilities. The researchers did, however, uncover one minor security problem: The client does not check one particular certificate when talking to other Dropbox clients on a local network. This potentially enables attackers to block the client of other network users. Source: <http://www.h-online.com/security/news/item/Worth-Reading-Dropbox-is-quite-secure-1747744.html>

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

44. *November 12, Colorado Springs Gazette* – (Colorado) **Skunk spray downs Fox 21 News for a day.** An almost day-long outage for KXRM 21 Colorado Springs and KXTU 20 Colorado Springs was apparently caused by a skunk that was burned inside the transmitter station, the Colorado Springs Gazette reported November 12. The wounded animal released his spray, soaking the transmitter and causing the breaker switch to be tripped inside, according to the station's Facebook page. The outage started November 11 and affected viewers using Dish, Direct TV, and those using antennas. Engineers spent the day at the Cheyenne Mountain station trying to dry it off and get the transmitter back up and running. Programming began again November 12. Source: <http://www.gazette.com/news/viewers-147230-signal-fox.html>
45. *November 12, WBNG 12 Binghamton* – (New York) **Phone lines down in Westford.** A severed phone line left a majority of residents in Otsego County, New York, without phone service, including the ability to call 9-1-1. Otsego County Emergency Services reported November 11 that the main phone line providing service to the Town of Westford was cut. The damaged line left most of the town without phone service. Verizon repair crews were notified and there was no estimated restoration time. Otsego County Emergency Services reminded residents the outage did not affect cell phone service in the area and that cell phones could be used to report emergencies. Source: <http://www.wbng.com/news/local/Phone-Lines-Down-in-Westford-178896081.html>

[\[Return to top\]](#)

Commercial Facilities Sector

46. *November 12, Hornell Evening Tribune* – (New York) **Investigators looking into cause of Rose Apartments explosion.** Two tenants were taken to the hospital, but no fatalities were reported in a November 11 explosion at Rose Apartments in Alfred, New York. Neither person's injuries were life-threatening, the Alfred Police Chief and County Fire Coordinator said. Police had a list of tenants and were working to account for all of them. Rose Apartments includes 40 one-bedroom units. The police chief said a preliminary investigation was underway, but that there was no evidence that any chemicals or a methamphetamine lab were factors. There were reportedly 35 people living in the building. The Red Cross responded and a temporary shelter was being set up at Alfred State College's Pioneer Center.

Source: <http://www.eveningtribune.com/topstories/x35737865/Investigators-looking-into-cause-of-Rose-Apartments-explosion>

47. *November 12, Charlotte Observer* – (North Carolina) **Official: Fire in Matthews caused more than \$250,000 in damage.** An apartment fire in Matthews County, North Carolina, that started from a first floor kitchen, caused between \$250,000 and \$300,000 in damage, said the Assistant Matthews Fire Chief, the Charlotte Observer reported November 12. However, a town spokeswoman said the department is still calculating a final damages estimate. Two people were injured November 9 in the three-alarm fire that damaged 23 apartment units in Matthews. Fire officials said two people were injured, apparently when they jumped from third-floor balconies in the three-story building. Medics reported that one person suffered life-threatening injuries, and the other person's injuries were described as non-life-threatening.

Source: <http://www.charlotteobserver.com/2012/11/12/3660735/official-fire-in-matthews-cost.html>

48. *November 12, WCMH 4 Columbus* – (Ohio) **Dozens of OSU students displaced after campus-area apartment fire.** Dozens of students in Columbus, Ohio, were displaced after a fire at a campus-area apartment building November 12. Upon arrival, firefighters upgraded the fire to a second alarm. It took firefighters about an hour to contain the fire. Wind complicated the firefighting effort. Fire officials said all occupants of the apartment building evacuated safely after smoke detectors went off. Approximately 25 to 30 students were displaced by the fire. Residents were permitted to return to their apartments November 12 to obtain basic belongings. The damage to the structure totaled approximately \$200,000, according to Columbus fire officials. The fire appeared to be accidental and most likely started in the rear of one of the units. North Fourth Street was blocked just south of Iuka Avenue by fire equipment while crews worked to contain the fire.

Source: <http://www2.nbc4i.com/news/2012/nov/12/10/red-cross-called-osu-students-after-2nd-alarm-fire-ar-1237777/>

49. *November 12, WBOC 16 Salisbury* – (Maryland) **Firefighter injured battling Cambridge blaze.** Authorities said a firefighter was hurt while battling a November 11 fire that heavily damaged a business in downtown Cambridge, Maryland. The Maryland Fire Marshal's Office said the blaze broke out at Jeni's Odds & Ends. It took 50 firefighters from the Rescue (Cambridge), Church Creek, Linkwood, Trappe, Oxford, and East New Market fire companies approximately an hour to get the two-alarm fire under control. Investigators said one firefighter suffered a minor injury after falling through a second-story floor during fire suppression. There were no other reported injuries. The fire reportedly caused an estimated \$100,000 in damage to the structure and \$10,000 in damage to its contents. Deputy State Fire Marshals determined the fire started in the interior of the second floor.

Source: <http://www.wboc.com/story/20072053/firefighter-injured-battling-cambridge-blaze>

50. *November 11, Las Vegas Sun* – (Nevada) **Warehouse fire damage estimated to be \$1 million.** A two-alarm fire November 11 caused an estimated \$1 million in damage to a

Universal Watch Co. building near Tropicana Avenue and Valley View Boulevard, said a spokeswoman for Clark County, Nevada. The first responding fire crew reported heavy smoke and flames and requested a second alarm. The roof of the warehouse portion of the building collapsed shortly after the first crew arrived. Fifty crew members and 18 units from Clark County Fire Department and Las Vegas Fire and Rescue battled the fire for about 30 minutes.

Source: <http://www.lasvegassun.com/news/2012/nov/11/warehouse-fire-causes-estimated-1-million-damage/>

[\[Return to top\]](#)

National Monuments and Icons Sector

51. *November 12, Winston-Salem Journal* – (North Carolina) **200 acres burned.** A wildfire at Pilot Mountain State Park in Surry County, North Carolina, burned 200 acres and was only 20 percent contained November 10, authorities said. Firefighters completed a 15 mile-long encirclement or fire-containment line, said the public-information officer for the North Carolina Division of Parks and Recreation. The fire began as a controlled burn intended to reduce underbrush fire hazards in about 180 acres, but it jumped the fire line after about 70 acres had been cleared.

Source: <http://www.fireengineering.com/news/2012/11/12/200-acres-burned.html>

[\[Return to top\]](#)

Dams Sector

52. *November 12, Associated Press* – (Louisiana) **Feds: Levee system did not cause Isaac flooding.** Federal officials said in a report released November 9 that improvements to the New Orleans-area levee system did not cause Hurricane Isaac's storm-surge flooding of areas in Louisiana that were not inundated during Hurricanes Katrina and Gustav. The Army Corps of Engineers said surge flooding during Isaac was the result of the storm's landfall just west of the Mississippi River, rainfall amounts of 8 to 20 inches, a forward speed three to four times slower than Katrina, and an extended period of easterly winds that pushed surge heights to record levels. The study found the unusual combination of Isaac's storm characteristics resulted in surge heights greater than those typically associated with a Category 1 hurricane. The study used two computer model simulations of Hurricane Isaac's storm surge to test whether it was affected by the levee system, one with the completed levee improvements, the other without the improvements.

Source: <http://www.insurancejournal.com/news/southcentral/2012/11/12/270230.htm>

[\[Return to top\]](#)



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)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.