Daily Open Source Infrastructure Report
3 October 2012

Top Stories

- Some 39 people on an Amtrak passenger train were injured when it derailed after a big rig crashed into it near Hanford, California, October 1. – *Associated Press* (See item **11**)
- American Airlines said passenger seats on a third flight in 1 week came loose as the plane was airborne, and that it was continuing to inspect other jets with similar seating. – *Associated Press* (See item **12**)
- A beef recall by XL Foods, Inc.of Alberta, Canada, expanded for the 13th time. It now has affected U.S. retailers in 41 States, and has rendered more than 1,100 beef products unsafe. – *Food Safety News* (See item **15**)
- A salmonella outbreak that has left hundreds of people sick in the Netherlands and the United States was traced to smoked salmon. – *Associated Press; CBS News* (See item **16**)
- A U.S. Border Patrol agent was killed and another wounded in a shooting October 2 in Naco, Arizona, near the U.S.-Mexico line. – *Associated Press* (See item **37**)

Fast Jump Menu

Energy Sector

1. *October 2, West Virginia Public Broadcasting* – (West Virginia) **Drilling activity resumes at site of August gas well explosion.** The West Virginia Department of Environmental Protection (DEP) has allowed drilling to resume at the site of a gas well explosion in August. The operator is required to give the agency more data on the site. The DEP is allowing Antero Resources, of Denver, the operator of the well, to resume vertical drilling at the Marcellus Shale well in Harrison County. But the company is not doing horizontal drilling work, because a new rig must be brought in to do that. In August, a fire occurred at the Cottrill No. 3 Well, injuring three workers and inflicting substantial damage to the drilling rig. The DEP spokesman said the company is also required to gather data on five residential water wells, within 2000 feet of the well. The company is testing for Total Dissolved Solids as well as a plethora of other compounds including, aluminum, iron, and arsenic. The DEP previously issued an order of violation to Antero because of the incident. Something caused methane to ignite as the rig was being removed from the well.
   Source: http://www.wvpubcast.org/newsarticle.aspx?id=26808

For another story, see item **4**

[Return to top]

Chemical Industry Sector

2. *October 2, Products Finishing Magazine* – (National) **EPA issues significant new use rules for 107 chemicals.** The U.S. Environmental Protection Agency (EPA) issued a direct final rule September 21 under the Toxic Substances Control Act (TSCA) for significant new uses of 107 different chemical, Products Finishing Magazine reported October 2. Published in the Federal Register, the rule requires those who intend to manufacture, import, or process any of these chemicals for new significant uses to notify EPA at least 90 days before commencing that activity. EPA will then evaluate the intended use and, if necessary, prohibit or limit the activity before it occurs. The rule covers many substances, including eight already subject to risk-based consent orders under TSCA section 5(e), requiring protective measures to limit exposures or otherwise mitigate potential unreasonable risk. Interested parties may submit written adverse or critical comments to any of the significant new use rules until October 22.
   Source: http://www.pfonline.com/news/epa-issues-significant-new-use-rules-for-107-chemicals

3. *October 1, Kansas City Business Journal* – (Missouri) **Bayer CropScience will pay penalty tied to misbranded pesticides.** Bayer CropScience LP will pay a civil penalty to settle violations tied to distributing misbranded pesticides from its Kansas City, Missouri facility. The Environmental Protection Agency (EPA) said October 1 that Bayer CropScience would pay $13,900 to the United States. An administrative consent agreement and final order filed by the local EPA office said a November inspection at the facility found that the pesticide Ethosumesate was shipped without a product label,

EPA registration number, or EPA producing establishment number. A label Bayer CropScience provided for two shipments of an unregistered pesticide — to be turned into a registered product — displayed false or misleading directions-for-use information, the EPA said. Bayer CropScience was required to relabel all the shipments in question and change its practices to prevent such violations in the future.
Source: http://www.bizjournals.com/kansascity/news/2012/10/01/bayer-cropscience-will-pay-penalty.html

For another story, see item **13**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *October 2, Nuclear Street* – (Florida) **Report: Cost of Crystal River 3 concrete repair likely to exceed Progress Energy estimates.** An outside analysis of concrete delamination at Crystal River, Florida's Crystal River nuclear plant concluded that repair costs would likely go beyond Progress Energy's initial estimates, to between $1.5 billion and $3.4 billion, Nuclear Street reported October 2. The review filed with the Florida Public Service Commission by Zapata Inc. reported that the current repair plan appears technically feasible, but challenges remain. While Progress' earlier estimates for repair costs topped out at $1.3 billion, the new study estimated they would run closer to $1.5 billion. Factoring in potential unplanned contingencies, Zapata also provided cost estimates for more extensive repairs. They included a worst-case scenario requiring replacement of the dome and the lower elevations. Should that happen, repairs would cost an estimated $3.4 billion and take 8 years. The reactor has been offline since 2009 when the wall of its containment building was found to be cleaving apart following a steam generator replacement. The plant's owner has not decided whether to repair or retire the plant.
Source:
http://nuclearstreet.com/nuclear_power_industry_news/b/nuclear_power_news/archive/2012/10/02/report_3a00_-cost-of-crystal-river-3-concrete-repair-likely-to-exceed-progress-energy-estimates-100202.aspx

5. *October 2, Global Security Newswire* – (National) **Authorities in U.S. drill responses to 'dirty bomb' strikes.** The United States the week of September 24 wrapped up a group of exercises in which national, State, and jurisdictional authorities weighed potential reactions to a hypothetical crisis involving multiple radiological "dirty bombs," the National Nuclear Security Administration (NNSA) announced. The last "Amber Waves 2012" drill enabled government personnel to address matters concerning the assumption of administrative powers held by the interagency Federal Radiological Monitoring and Assessment Center during mitigation activities following a radiological strike, according to an NNSA press release. The Environmental Protection Agency's possible oversight of regions affected by harmful materials was another focus at the gathering. Kansas and Missouri hosted the Amber Waves 2012 events, which considered a potential attack incorporating synchronized dirty-bomb

strikes in Leavenworth County, Kansas, and Kansas City, Missouri.
Source: http://www.nti.org/gsn/article/us-authorities-drill-dirty-bomb-strikes/

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

6. *October 1, Los Angeles City News Service* – (California) **EPA fines Corona company for alleged clean air violations.** A Corona, California-based battery manufacturer was fined $167,300 for failing to comply with federal emission control regulations, the U.S. Environmental Protection Agency (EPA) announced October 1. U.S. Battery, which makes batteries for everything from golf carts to tanks, was assessed the penalty by the EPA for violating provisions of the Clean Air Act, according to the federal agency. According to the EPA, an investigation of the company's pollution-monitoring practices was initiated in February 2010 and revealed U.S. Battery was not conducting semi-annual inspections of its filtering equipment, nor keeping any records to confirm the performance of routine maintenance. As part of the EPA action, U.S. Battery agreed to voluntarily install "High-Efficiency Particulate Air" filters to reduce lead acid emissions, in addition to using existing pollution control equipment at the Corona plant, which has been operational since 1991.
Source: http://www.swrnn.com/2012/10/01/epa-fines-corona-company-for-alleged-clean-air-violations/

[Return to top]

Banking and Finance Sector

7. *October 1, Ars Technica* – (International) **DSL modem hack used to infect millions with banking fraud malware.** Millions of Internet users in Brazil fell victim to a sustained attack that exploited vulnerabilities in DSL modems, forcing people visiting sites such as Google or Facebook to reach imposter sites that installed malicious software and stole online banking credentials, a Kaspersky security researcher said. The attack, described the week of September 24 during a presentation at the Virus Bulletin conference in Dallas, infected more than 4.5 million DSL modems, said the researcher, citing statistics provided by Brazil's Computer Emergency Response Team. The cross-site request forgery (CSRF) vulnerability allowed attackers to use a simple script to steal passwords required to remotely log in to and control the devices. The attackers then configured the modems to use malicious domain name system servers that caused users trying to visit popular Web sites to instead connect to booby-trapped imposter sites.

Source: http://arstechnica.com/security/2012/10/dsl-modem-hack-infects-millions-with-malware/

8. *October 2, Softpedia* – (International) **Persistent flaws in PayPal allow cybercriminals to hijack user sessions and more.** Multiple Web vulnerabilities have been identified by Vulnerability Lab researchers on the official PayPal Web site, Softpedia reported October 2. The high-severity security holes could have been exploited by a remote attacker against Pro, seller, or regular customer accounts. "A persistent input validation vulnerability is detected in the official Paypal ecommerce website content management system (Customer/Pro/Seller). The bugs allow remote attackers to implement/inject malicious script code on the application side (persistent) of the paypal web service," the experts explained. "The vulnerability is located in the company profile input fields with the bound vulnerable address_id, details (mail) & companyname parameters. The bug affects the important user profile listing, the address listings & security notification (mail)," they added. A similar vulnerability also affects the mail security notification module. If exploited successfully, the flaws could have allowed a cybercriminal to hijack user sessions, steal accounts via persistent Web attacks, and manipulate context in the affected modules. According to the experts, the payment processor was notified of the issues in July, but the security holes were addressed only in mid-September.
Source: http://news.softpedia.com/news/Persistent-Flaws-in-PayPal-Allow-Cybercriminals-to-Hijack-User-Sessions-and-More-296107.shtml

9. *October 1, Agence France-Presse* – (National) **Scam went back further than thought.** The Bernard L. Madoff Investment Securities LLC's multi-billion dollar Wall Street fraud, the largest in U.S. history, started in the early 1970s, at least two decades earlier than previously thought, officials said October 1. The revelation was contained in a superseding indictment that adds charges against five former employees of the investment firm who are accused of conspiring to defraud clients of billions. The alleged new crimes in the indictment include bank fraud charges and tax offenses, the federal prosecutor's office in Manhattan, New York said. "Whereas the November 2010 Indictment alleged that the conspiracy to defraud BLMIS's clients began in or about 1992, the Superseding Indictment dates the conspiracy back to at least the early 1970s," the prosecutor's office said in a statement. A FBI official said the five defendants were "at the core" of the scheme. Shielded by a reputation as one of Wall Street's most savvy investors, the firm's leader secretly stole clients' capital to pay back steady returns in phony profits. The scheme only collapsed in 2008 amid the U.S. financial crisis.
Source:
http://www.google.com/hostednews/afp/article/ALeqM5gDs6GNYPoPWPNgz-SKZgGX-TRWiw?docId=CNG.4f566a1bee1ffb2806d0dacbf247b94d.561

10. *October 1, Associated Press* – (Kentucky; New York) **Federal authorities in NY charge Ky. man and 2 others in $100M fraud linked to bank collapse.** A Kentucky businessman was arrested October 1 in a $100 million scheme that contributed to the collapse of a bank and tried to drain money from the federal bank bailout program before some funds were used to pay his mortgages and to buy luxury goods, authorities

said. Along with two alleged accomplices arrested in New York, the man faces various charges, including conspiracy to commit bank bribery, bank and insurance fraud, and tax evasion. A U.S. attorney in New York City alleged that the man carried out several illegal financial schemes that relied largely on his corrupt relationship with New York's Park Avenue Bank, its former president, and the bank's senior vice president. The former president previously pleaded guilty to fraud, bank bribery, embezzlement, and conspiracy. The bank's senior vice president also was arrested, along with the executive director of investments at an investment bank and financial services company headquartered in Manhattan. The government said the executive director also aided the Kentucky man in his schemes.
Source: http://www.washingtonpost.com/business/federal-authorities-in-ny-charge-ky-man-and-2-others-in-100m-fraud-linked-to-bank-collapse/2012/10/01/fe19125c-0bf8-11e2-97a7-45c05ef136b2_story.html

For another story, see item **38**

[Return to top]

Transportation Sector

11. *October 2, Associated Press* – (California) **Amtrak: Crossing gate down in Calif. train crash.** The crossing gate was down, lights were flashing and bells were ringing when a big rig crashed into a passing Amtrak passenger train October 1 near Hanford, California, an Amtrak official said. An Amtrak spokeswoman said 39 people on the train from Oakland to Bakersfield were injured. The truck hit the train being pushed by the locomotive between the locomotive and the last car. Authorities described the injuries as mostly bumps and bruises, although the spokeswoman said at least one person suffered a broken leg. The driver of the big rig went through the warning arms and hit the train before his truck overturned, according to the California Highway Patrol (CHP). The impact from the truck pushed two of the train's four cars and its locomotive off the tracks. The train traveled about 600 feet after the collision before hitting a switchback and derailing, the CHP said. Officials have not determined how fast the train or the truck were going, but the average speed for Amtrak through the area is 70 mph to 80 mph, while the speed limit on the roadway where the truck was traveling is 55 mph, according to the CHP. The track reopened October 2 after crews replaced hundreds of feet of damaged track and some signal equipment, a BNSF Railway spokeswoman said. BNSF owns the line.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5gWG0sV284DbFwiKeZppdTCOv7EIA?docId=e163a35665544b2fb6e9bb7a34faf434

12. *October 2, Associated Press* – (National) **American Airlines inspects jets after passenger seats break loose in mid-flight on 3 planes.** American Airlines said passenger seats on a third flight came loose as the plane was airborne, and it was continuing to inspect other jets with similar seating. The airline acknowledged October 2 that seats came loose on a flight the week of September 24 between Vail, Colorado, and Dallas-Fort Worth International Airport in Texas. The same thing happened on a

flight September 29 and another October 1. An American Airlines spokeswoman said the airline is inspecting eight of its Boeing 757s that share similar seat assemblies. An initial review by American indicated that there could be a problem with the way the seats fit into tracks on the floor of the Boeing 757, but technical teams from the airline "are looking at everything," she said. The planes involved in the incidents were recently worked on at an American Airlines maintenance base in Tulsa, Oklahoma, and a Timco Aviation Services facility in North Carolina. The Federal Aviation Administration said it is looking into the incidents.
Source: http://www.washingtonpost.com/business/american-airlines-will-inspect-several-planes-after-seats-come-loose-on-at-least-2-jets/2012/10/01/7733e732-0c28-11e2-97a7-45c05ef136b2_story.html

13. *October 2, WSFA 12 Montgomery* – (Alabama) **I-85 and I-65 traffic blocked overnight.** All lanes of traffic on I-85 were opened October 2 after a tractor trailer started leaking a hazardous chemical near the Tuskegee exit October 1 in Montgomery, Alabama shut down all lanes of the highway for many hours. The substance was believed to be silicone tetra fluoride. The spill was cleared. I-65 was also re-opened October 2 after a vehicle fire caused one northbound and one southbound lane to be blocked overnight near the Hyundai Boulevard exit. A small U-Haul truck carrying approximately 100 gallons of paint and adhesive caught fire. The fire was contained to the cab of the truck and did not damage the cargo in the rear of the truck.
Source: http://www.wsfa.com/story/19703795/i-85-and-i-65-overnight-accidents

14. *October 2, CNN* – (Illinois; International) **American Airlines plane makes emergency landing.** An American Airlines flight from Chicago to London made an unscheduled landing October 2 at Shannon Airport in Ireland after a passenger reported a smoky odor, an airline spokesman said. American Airlines Flight 98, a Boeing 777-200 carrying 246 passengers and 14 crew members, was diverted as a precaution, he said. An inspection revealed the odor was coming from an overhead fan that had overheated, the spokesman noted. The head of operations for Shannon Airport said such technical diversions are not uncommon.
Source: http://www.cnn.com/2012/10/02/travel/american-airlines-problem/index.html?hpt=hp_t3

For another story, see item **47**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

15. *October 2, Food Safety News* – (International) **Canadian beef recall grows, again.** October 2, Food Safety News reported the thirteenth expansion of the XL Foods, Inc. recall. Alberta, Canada-based XL Foods, Inc. is voluntarily recalling 260 more varieties of beef, announced the Canadian Food Inspection Agency in a health alert October 1. These newly recalled meats have been added to hundreds of other beef products recalled by the company in the past 2 weeks. Some beef products listed in this latest recall — including rump roast, soup bones, and tenderized hip steak among others — were not listed in previous recall updates that have mainly included ground beef and various whole and tenderized cuts. Products affected by this update were manufactured on the same dates as XL's previously recalled ground beef products — August 24, 27, 28, 29, and September 5. Affected products were sold in retail stores across the United States, including Dominion, Extra Foods, Real Atlantic, Save Easy, ValuFoods, Valu-mart, VillageMart, and Zehrs, among others. The XL Foods recall has so far affected U.S. retailers in 41 States, and has rendered over 1,100 beef products unsafe.
Source: http://www.foodsafetynews.com/2012/10/canadian-beef-recall-grows-again/#.UGru7pGvMcs

16. *October 2, Associated Press; CBS News* – (International) **Salmonella tied to Dutch salmon sickens hundreds.** A salmonella outbreak that has left hundreds of people sick in the Netherlands and the United States was traced to smoked salmon, CBS News reported October 2. The Netherlands' National Institute for Public Health and the Environment (RIVM) said the salmon was traced to Dutch company Foppen, which sells fish to many major Dutch supermarkets and to stores around the world, including the United States. RIVM said that around 200 people — and likely more — in the Netherlands, and more than 100 people in the United States were sickened. A RIVM spokesman said the institute got its information on Americans becoming ill from the Centers for Disease Control and Prevention (CDC). However, a CDC representative said the agency had not confirmed any illnesses. A Foppen company spokesman said that in the United States, Foppen sells only to Costco Wholesale Corp., which would deal with any U.S. recall. The smoked salmon was sold under the Foppen name, as well as under Costco's store-brank name, Kirkland. Costco said it had no reports of illness.
Source: http://www.cbsnews.com/8301-204_162-57524385/salmon-based-salmonella-outbreak-sickens-hundreds/

17. *October 1, Homeland Security News Wire* – (National) **Probability maps help detect food contamination.** October 1, Homeland Security News Wire reported that Sandia National Laboratories' National Infrastructure Simulation and Analysis Center published a study in the International Journal of Critical Infrastructures, which demonstrates how developing a probability map of the food supply network using stochastic network representation might shorten the time it takes to track down contaminated food sources. Stochastic mapping shows what is known about how product flows through the distribution supply chain and provides a means to express all the uncertainties in potential supplier-customer relationships that persist due to incomplete information. If used on a larger scale, such methods also might assess the

vulnerability of food supplies to wide-scale, deliberate contamination.
Source: http://www.homelandsecuritynewswire.com/dr20121001-probability-maps-help-detect-food-contamination

18. *September 30, Food Poisoning Bulletin* – (National) **Fresh Express recalls expired Hearts of Romaine Salad.** Fresh Express recalled another variety of Romaine salad for possible Listeria monocytogenes contamination, Food Poisoning Bulletin reported September 30. The new recall is for expired packages of 18-ounce Hearts of Romaine Salad with the expired use by date September 26 and product code H256808. One package of the product tested positive for Listeria as part of a random sample test. The product was sold in the northwest and midwest United States. The week of September 24, Fresh Express recalled 9-ounce packages of Leafy Green Romaine Salad.
Source: http://foodpoisoningbulletin.com/2012/fresh-express-recalls-expired-hearts-of-romaine-salad/

19. *September 28, U.S. Food and Drug Administration* – (National) **Newman's Own Organics issues a limited voluntary recall of their Peanut Butter Newman-O's Sandwich CrÃ¨me Cookies because of health risk.** The U.S. Food and Drug Administration reported September 28 that Newman's Own Organics announced a voluntary limited recall of certain lots of Peanut Butter Newman-O's Sandwich CrÃ¨me Cookies because the products may be contaminated with Salmonella. Package expiration dates include May 3 and May 27, 2013. This recall is due to the expanded scope of Sunland, Inc.'s recall of nut butter products. The cookies were distributed nationwide via retail stores. No other Newman's Own Organics products or expiration dates are affected by this recall.
Source: http://www.fda.gov/Safety/Recalls/ucm322107.htm

[Return to top]

Water Sector

20. *October 2, WZZM 13 Grand Rapids* – (Michigan) **Boil water in area of Ada Township.** Residents in a portion of Ada Township, Michigan were given a boil water order because of possible bacterial contamination, WZZM 13 Grand Rapids reported October 2. Township leaders said the water system lost pressure because of a line break on Rix Street. The area where the boil water advisory is in effect is the Ada Village proper and the Adatown neighborhood. The leaders advised residents to boil their water for at least 1 minute before it is used, or to use bottled water. The township water staff plans to flush the system and test for contamination. The boil order would remain in effect until the water was verified as clean.
Source: http://www.wzzm13.com/news/article/227362/2/ADVISORY-Boil-water-in-Ada-Township

21. *October 2, Associated Press* – (Pennsylvania) **Pa. township official charged with sewage releases.** A township official responsible for running a sewage treatment plant in James City, Pennsylvania was charged with releasing about 10 million gallons of raw sewage into nearby waterways, the Associated Press reported October 2. The

suspect was chairman of the Highland Township supervisors in Elk County, and the only certified sewage treatment plant operator at the facility owned by the Highland Township Municipal Authority. Attorney general's investigators said he falsified records then made false statements to agents who investigated the alleged sewage releases into a tributary leading to Wolf Run. Authorities also determined the plant was actually being operated by a non-certified trainee instead of the township official, who faced a preliminary hearing set for October 3.
Source: http://www.ydr.com/state/ci_21679422/pa-township-official-charged-sewage-releases

22. *October 2, Lafayette Daily Advertiser* – (Louisiana) **Tank explosion underscores consumer water complaints.** Residents of Windy Meadows and Country Village in Youngsville, Louisiana, were left without water for more than 2 days, the Lafayette Daily Advertiser reported October 2. The neighborhood water tank, which is owned and operated by Total Environmental Solutions Inc. (TESI) was found September 30 to have a large gaping hole in the middle. A new water tank was delivered October 1 and was scheduled to be installed, stated the TESI Web site. Residents were asked to continue boiling their water before consumption until further notice. About 6,200 residents across Lafayette Parish, from Youngsville to Carencro, receive water from TESI. For 11 of the last 12 quarters, the TESI source in Windy Meadows was not in compliance with the Environmental Protection Agency. TESI has several unresolved violations, including management practices with sewage and maintenance, permit violations, discharge, and improper or incorrect reporting.
Source: http://www.theadvertiser.com/article/20121002/NEWS01/210020315/Tank-explosion-underscores-consumer-water-complaints?odyssey=tab|topnews|text|FRONTPAGE

23. *October 1, KATV 7 Little Rock* – (Arkansas) **Mayflower water system under boil order.** The residents in Mayflower, Arkansas, were issued orders to boil their drinking water until further notice. A spokesperson for the city of Mayflower said October 1, the "entire system is down" due to a break in a water main. Workers were expected to have the water flowing again within a few hours, but because of the possibility of contamination, water for human consumption should be boiled at least 5 minutes before drinking.
Source: http://www.katv.com/story/19688667/mayflower-water-system-under-boil-order

24. *October 1, Bluefield Daily Telegraph* – (West Virginia) **Boil water advisories issued for four Mercer County communities.** The West Virginia Department of Health and Human Resources (DHHR) reissued boil water advisories for four different Mercer County communities, the Bluefield Daily Telegraph reported October 1. A boil water advisory was reissued for the Weyanoke Giatto Water System in Matoaka, the Pinnacle Water Association in the McComas area, the Windmill Gap Water System in Rock, and the Hiawatha Water Association in Hiawatha. According to the DHHR, the systems were under boil water advisories for failure to properly monitor drinking water and the lack of a properly certified operator. No date was given for when the advisories will be lifted.

Source: http://bdtonline.com/local/x1241988990/Boil-water-advisories-issued-for-four-Mercer-County-communities

25. *October 1, San Antonio Business Journal* – (Texas) **SAWS crews contain sewer spills in northwest San Antonio.** Heavy rains the weekend of September 29 triggered several sewer spills along Leon Creek in San Antonio. The San Antonio Water System (SAWS) announced September 30 that crews responded to a sewer spill near State Highway 151 just east of Military Drive West along Leon Creek. However, October 1 SAWS announced crews spotted an additional sewer spill 1 mile upstream from the original spill. SAWS estimated both spills released more than 100,000 gallons of wastewater into the environment. Since then, crews have contained both spills. SAWS said it did not appear that the two sewage spills had a long-term effect to the area because of the heavy rains. However, officials said they would continue to monitor the area.
Source: http://www.bizjournals.com/sanantonio/news/2012/10/01/saws-crews-contain-sewer-spills-in.html

For another story, see item **1**

[Return to top]

Public Health and Healthcare Sector

26. *October 2, WCTI 12 New Bern* – (North Carolina; Tennessee) **State health director warns of meningitis outbreak.** The North Carolina Department of Health and Human Services (DHHS) was assisting the Centers for Disease Control and Prevention (CDC) in investigating a meningitis outbreak involving patients treated with spinal steroid injections at outpatient surgical centers and pain management clinics, WCTI 12 New Bern reported October 2. One patient was identified in North Carolina and 11 more, including two patients that died, were identified from one clinic in Tennessee. The form of meningitis in the patients was suspected to be Aspergillus. The source for the outbreak was not yet known. DHHS' Division of Public Health was working with outpatient facilities to contact all North Carolina patients who received epidural steroid injections since July 1, 2012 using the same medication used in the Tennessee clinic.
Source: http://www.wcti12.com/news/State-Health-Director-warns-of-Meningitis-outbreak/-/13530444/16813768/-/i8qfad/-/index.html

27. *October 2, Associated Press* – (Maine; Virginia) **Maine doctor settles federal billing complaint.** Authorities said a Maine doctor agreed to pay more than $321,000 to settle claims that he falsely billed federal health care programs, the Associated Press reported October 2. Federal prosecutors said the osteopathic physician, with offices in Freeport, Maine, and Alexandria, Virginia, agreed to pay back money he billed Medicare and Tricare for providing osteopathic manipulative treatment, evaluation, and management services to patients in violation of billing guidelines. Authorities said the false billing took place from October 2004 through June 2011.
Source: http://www.wgme.com/template/inews_wire/wires.regional.me/254aaf5f-www.wgme.com.shtml

28. *October 2, Becker's Hospital Review* – (Wyoming) **Wyoming Medical Center agrees to $2.7M settlement for alleged medicare fraud.** Wyoming Medical Center (WMC) in Casper, Wyoming, agreed to pay $2.7 million to settle Medicare fraud allegations stemming from a 2007 whistleblower suit, Becker's Hospital Review reported October 2. A former WMC employee alleged that WMC submitted reimbursement requests that were inconsistent with patients' treatment records, changed the admission status of patients from outpatient to inpatient status without a physician order, and billed Medicare for unnecessary admissions. The government conducted an investigation into the hospital, finding evidence to support some of the claims. WMC's settlement specifically resolves claims it submitted inpatient claims to Medicare for services performed in outpatient settings, inpatient claims for hospital stays for which there was no record of a physician ordering inpatient-level care, and inpatient claims for patients who did not meet inpatient admission requirements.
Source: http://www.beckershospitalreview.com/legal-regulatory-issues/wyoming-medical-center-agrees-to-27m-settlement-for-alleged-medicare-fraud.html

29. *October 1, South Florida Sun-Sentinel* – (Florida) **Weston doctor imprisoned for healthcare fraud in Boca Raton, Fort Lauderdale.** A psychiatrist was sentenced to 10 years in federal prison and ordered to pay more than $51.9 million in restitution October 1 for his role in what prosecutors called "one of the largest and most brazen health care fraud conspiracies in recent memory." The psychiatrist, who practiced in Fort Lauderdale and Boca Raton, Florida, was found guilty of conspiracy to commit health care fraud earlier in 2012. Prosecutors said he was part of a broader conspiracy involving American Therapeutic Corp. (ATC), which billed the taxpayer-funded Medicare program for more than $205 million in fraudulent claims. "This massive fraud was committed by manipulating the proper treatment of Alzheimer's and dementia patients, substance abusers seeking treatment, and others convinced or cajoled into spending time at ATC," the prosecutor wrote in court documents. A second south Florida psychiatrist of Coral Gables was also sentenced to 10 years in federal prison for his role in the fraud conspiracy. He was ordered to pay more than $87.4 million in restitution. More than 30 defendants have been charged and more than half have pleaded guilty or been convicted at trial, prosecutors said. ATC's six clinics in south Florida were shut down in 2010. The fraud went on for 8 years and involved hundreds of employees and associates, court records say.
Source: http://articles.sun-sentinel.com/2012-10-01/news/fl-broward-doctor-sentencing-20121001_1_health-care-fraud-weston-doctor-fraudulent-claims

[Return to top]

Government Facilities Sector

30. *October 2, Dark Reading* – (International) **Team GhostShell exposes 120,000 records from universities.** The hacktivist group TeamGhostShell says it has embarked on a new campaign to expose data and vulnerabilities at 100 of the top universities around the world. In a posting on Pastebin October 1, TeamGhostShell released 120,000 records from universities such as Oxford and Harvard. The campaign, which the group has dubbed "Project WestWind," has revealed vulnerabilities in university systems that

could put hundreds of thousands more records at risk, the group says. "We tried to keep the leaked information to a minimum, so just around 120,000+ accounts and records are here, leaving in their servers hundreds of thousands more," the group states. "When we got there, we found out that a lot of them have malware injected. No surprise there, since some have credit card information stored." The group said its goal is to raise awareness of problems in the modern education system. The posting does not discuss how the data was obtained or how much data the group was able to expose.
Source: http://www.darkreading.com/identity-and-access-management/167901114/security/attacks-breaches/240008262/team-ghostshell-exposes-120-000-records-from-universities.html

31. *October 2, Rochester YNN* – (New York) **Fire at town and village offices in Castile.** An investigation was underway to determine the cause of a major October 2 fire that gutted a building housing the town and village of Castile, New York's court and clerk's office, as well as a restaurant and an apartment. Firefighters said the town and village were in a state of emergency because their governments cannot operate due to the fire. Firefighters believed that an apartment on the 2nd floor was where the fire started. They said the that nearly all records were taken out of the building; a major concern. Firefighters said 24 fire companies responded, and about nine remained on scene.
Source: http://rochester.ynn.com/content/top_stories/602548/fire-in-castile-may-have-destroyed-government-records/

32. *October 1, Associated Press* – (Washington, D.C.) **White House says 1 of its unclassified networks was cyberattacked, says effort was repelled.** The White House acknowledged an attempt to infiltrate its computer system, but said it thwarted the effort and that no classified networks were threatened, the Associated Press reported October 1. The White House Press Secretary told reporters in Henderson, Nevada, that the White House is equipped with mitigation measures that identified the attack, isolated it, and prevented its spread. He said there was no indication that any data was removed. "There are distinctions between those networks that contain classified information and those that don't, and the attack was against an unclassified network," he said. He described the attack as "spear-phishing" and said such efforts against government computer systems are "not infrequent."
Source: http://www.washingtonpost.com/politics/white-house-says-1-of-its-unclassified-networks-was-cyber-attacked-says-effort-was-repelled/2012/10/01/a4c4e5d0-0bc8-11e2-97a7-45c05ef136b2_story.html

33. *October 1, Fort Worth Star-Telegram* – (Texas) **Arlington man charged with trying to hire a hit man to kill federal judge.** An Arlington, Texas man who was already in federal custody on accusations of filing false tax returns was charged October 1 with trying to hire a hit man to kill a federal judge for $100,000, according to federal authorities. A federal inmate and a FBI agent posing as the hit man thwarted the plot the week of September 24, federal officials said October 1 in a news release. The plan called for the "killer" to position himself within the Burnett Plaza Building, across from the Federal Courthouse in Fort Worth, arm himself with a high-power rifle with a scope and shoot the judge when he entered the courthouse, a federal criminal complaint says.

If that plan did not work, the suspect wanted the killer to plant a bomb in the judge's vehicle. The suspect wanted the judge killed so he would not hear his tax case. Federal agents were tipped off to the plot September 12 by an inmate. The inmate told federal authorities the suspect claimed to be a sovereign citizen and was therefore immune from all laws of the United States.
Source: http://www.star-telegram.com/2012/10/01/4302253/arlington-man-charged-with-trying.html#storylink=cpy

34. *October 1, Orange County Register* – (California) **Newport's City Hall reopened after evacuation for suspicious backpack.** Authorities found what they describe as "miscellaneous personal items" inside a camouflaged backpack that prompted evacuation October 1 of the city hall in Newport Beach, California. Authorities had evacuated city hall after a city employee reported the backpack as suspicious, said a Newport Beach Police Department spokeswoman. The bag was between the city council chambers and the administration building. A voluntary evacuation was also in effect for nearby businesses on 32nd Street. The Orange County Sheriff's Department bomb squad assessed the bag and found it contained "miscellaneous personal items," the police spokeswoman said. Approximately 3 hours later, about 200 city employees were let back into city hall. Authorities took the backpack to the police department.
Source: http://www.ocregister.com/news/city-373235-lowe-suspicious.html

35. *October 1, KJRH 2 Tulsa* – (Oklahoma) **City of Tulsa investigation concludes personal information not accessed during hacking scare.** City of Tulsa, Oklahoma officials said personal information was not accessed during a hacking scare involving the city's Web site, KJRH 2 Tulsa reported October 1. Officials mailed around 90,000 letters, warning people their information may have been at risk after one of the main servers was thought to have been hacked, prompting the shutdown of the city's Web site. "We had to treat this like a cyber-attack because every indication initially pointed to an attack," said the city manager. Officials said a third-party firm contracted by the City of Tulsa's IT department periodically attempts to access the city's networks to identify vulnerabilities. An unfamiliar testing procedure was used, which was initially thought to have been a hacking attempt. The firm has confirmed no personal information was accessed. "[We] have used this opportunity to enhance our network security and strengthen processes that we would use to identify potential breaches," the mayor said. The incident cost the city about $20,000 to mail the warning letters to those potentially impacted.
Source: http://www.kjrh.com/dpp/news/local_news/city-of-tulsa-investigation-concludes-personal-information-not-accessed-during-hacking-scare

36. *September 30, Associated Press* – (Massachusetts) **Woman pleads guilty to sending threatening letters.** A New York State woman pleaded guilty September 27 to sending threatening letters containing harmless white powder to officials in Massachusetts. Federal prosecutors said she pleaded guilty to mailing four threatening communications. Two of the letters went to the offices of a Massachusetts U.S. Senator and the State attorney general. The others were sent to the State district court in Greenfield and the Franklin County House of Correction there. Prosecutors said the letters sent in May 2011 led authorities to temporarily close the offices where they were

received.
Source: http://boston.cbslocal.com/2012/09/30/woman-pleads-guilty-to-sending-threatening-letters-to-brown-coakley/

For another story, see item **45**

[Return to top]

Emergency Services Sector

37. *October 2, Associated Press* – (Arizona) **Border Patrol agent shot, killed on patrol in Ariz.** A U.S. Border Patrol agent was killed and another wounded in a shooting October 2 in Arizona near the U.S.-Mexico line, according to the Border Patrol. The agents were shot while patrolling on horseback in Naco, Arizona, October 2, the Border Patrol said in a statement. The agents who were shot were on patrol with a third agent, who was not harmed, according to the president of the National Border Patrol Council, a union representing about 17,000 border patrol agents. The shooting occurred after an alarm was triggered on one of the many sensors along the border and the three agents went to investigate, said a Cochise County Sheriff's spokeswoman. Authorities have not identified any suspects, she said. It is not known whether the agents returned fire. The wounded agent was airlifted to a hospital after being shot in the ankle and buttocks, the Border Patrol said. That agent was in surgery and expected to recover said the union president.
Source: http://www.myrtlebeachonline.com/2012/10/02/3092994/homeland-security-says-border.html

For more stories, see items **5** and **36**

[Return to top]

Information Technology Sector

38. *October 2, Softpedia* – (International) **Prolexic: 'itsoknoproblembro' DDoS attacks are highly sophisticated.** Experts from Prolexic Technologies claim a new type of distributed denial-of-service (DDoS) attack has not only increased in size, but also reached a new level of sophistication. DDoS attacks have recently caused a lot of problems for organizations; in September, the sites of several financial institutions were disrupted as a result of such operations. Prolexic found that many of the recent attacks against their customers relied on the itsoknoproblembro DDoS toolkit. By combining the toolkit's capabilities with other sophisticated methods, the cyber criminals have been able to launch attacks that are difficult to mitigate even for specialized firms. Prolexic recorded massive sustained floods, some of which peaked at 70 Gbps and over 30 million pps. Itsoknoproblembro includes a number of application layer and infrastructure attack vectors, such as UDP and SSL encrypted attack types, SYN floods, and ICMP. The botnet that powers these attacks contains a large number of legitimate IP addresses. This allows the attack to bypass the anti-spoofing mechanisms deployed by companies.

Source: http://news.softpedia.com/news/Prolexic-quot-itsoknoproblembro-quot-DDOS-Attacks-Are-Highly-Sophisticated-296180.shtml

39. *October 2, Softpedia* – (International) **Twitter authentication flaw allows hackers to hijack user accounts.** Cyber criminals can steal Twitter accounts by leveraging a flaw in the social network's authentication system. In a recent case, a hacker utilized software that repeatedly tests common passwords against the account. This type of brute force attack is possible because Twitter only limits the log-in attempts if they come from the same IP address. Most Web sites implemented a system that prevents potential criminals from hijacking accounts by trying out random passwords. However, since Twitter only prevents multiple log-in attempts from the same computer, attackers can try out as many passwords as they want as long as they change their IP address.
Source: http://news.softpedia.com/news/Twitter-Authentication-Flaw-Allows-Hackers-to-Hijack-User-Accounts-296206.shtml

40. *October 2, The H* – (International) **Internet Explorer security examined.** A security expert illustrated how different statistical approaches can provide differing perspectives on browser security. For example, if only vulnerabilities are counted, Internet Explorer compares well with its competitors. However, if vulnerabilities that are actually exploited are counted, Internet Explorer fares comparatively poorly, according to the researcher. He calculated that 275 vulnerabilities were reported for Google Chrome in 2011, 97 for Mozilla Firefox, and only 45 for Internet Explorer. Using this method, Internet Explorer appears to be have a solid security story. However, looking at the statistics for zero-day exploits actually spread by malicious Web sites, Internet Explorer ranks far behind other browsers. Between January 2011 and September 2012, the researcher counted 89 days on which Internet Explorer users were exposed to actively exploited security vulnerabilities, compared to none at all for either Google Chrome or Mozilla Firefox. The researcher argues that, "Active exploitation is the most important qualifier of a true zero-day." He believes this is what matters from a user perspective.
Source: http://www.h-online.com/security/news/item/Internet-Explorer-security-examined-1721876.html

41. *October 1, Help Net Security* – (International) **IEEE password compromise was due to proxy 'anomaly'.** The week of September 24, a researcher revealed that he found the usernames and passwords of 100,000 members of the Institute of Electrical and Electronics Engineers (IEEE) unencrypted on a FTP server, available for anyone to find. Upon being notified of the matter, the organization mounted an investigation, and revealed its results: "The incident related to the communication of user IDs and passwords between two specific applications within our internal network resulting in the inclusion of such data in web logs. An anomaly occurred with a process executed in coordination with a proxy provider of IEEE, with the result that copies of some of the logs were placed on our public FTP server. These communications affected approximately two percent of our users. The log files in question contained user IDs and accompanying passwords that matched our directory. The primary logs were, and are, stored in protected areas." IEEE made also sure to note that it does not store its corporate directory information in the clear, does not expose it to the public, and was

not compromised.
Source: http://www.net-security.org/secworld.php?id=13697

42. *October 1, Softpedia* – (International) **Quervar malware found to download ZeroAcess trojans and ransomware.** September 27, security researchers from Trend Micro spotted a new variant of the Quervar malware. Cyber criminals launched a new Quervar campaign paired with two different payloads: ZeroAccess trojans and ransomware. The ransomware is designed to lock computers and demand ransoms in the name of the FBI. The trojan, TROJ_SIREFEF.SZP, is a rootkit malware that hides its presence by patching the services.exe file, and by disabling all the operating system's security-related services.
Source: http://news.softpedia.com/news/Quervar-Malware-Found-to-Download-ZeroAcess-Trojans-and-Ransomware-295909.shtml

43. *October 1, The H* – (International) **SQL injection in Trend Micro's Control Manager.** Trend Micro's platform for centralized security management is vulnerable to SQL injection attacks. According to the U.S. Computer Emergency Readiness Team, versions 5.5 and 6.0 of the Trend Micro Control Manager are vulnerable. The company provided patches for both affected versions. The vulnerability in question concerns a blind SQL injection attack which means the Web frontend does not divulge any information from the database. According to a report by security consulting firm Spentera that includes a proof-of-concept, the vulnerable system can be made to leak information such as password hashes by analyzing the timing of SQL queries.
Source: http://www.h-online.com/security/news/item/SQL-injection-in-Trend-Micro-s-Control-Manager-1721385.html

For more stories, see items **7**, **8**, **30**, **32**, and **35**

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

Nothing to report

[Return to top]

Commercial Facilities Sector

44. *October 2, Toledo Blade* – (National) **Local mosque fire ruled arson.** Officials October 1 ruled a fire at the Islamic Center of Greater Toledo, Ohio as arson, but

remained tight-lipped about details. A Perrysburg Township police official said officers would likely be stationed outside the center 24 hours a day for many days. Neither police nor the State fire marshal commented on a motive for the fire. The Bureau of Alcohol, Tobacco, Firearms and Explosives was also investigating. A former long-time center administrator said he was told there was a report of smoke in the prayer area when the fire was reported September 30. He was also told there is considerable smoke and water damage inside the second-floor prayer room, partially, he added, from a sprinkler system.
Source: http://www.ourtownperrysburg.com/Police-Fire/2012/10/02/Local-mosque-fire-ruled-arson.html

45. *October 2, Livingston Daily* – (Michigan) **Fire damages Byron businesses.** An October 1 fire gutted most of a downtown Byron, Michigan commercial block, including a restaurant, the apartments above it, and other nearby businesses, authorities said. Firefighters from 11 departments responded to the fire on South Saginaw Street. The cause of the fire was under investigation, but it was believed to have started in an apartment above Janelle's Family Restaurant. Other businesses affected include New Image salon, a hardware store, and a resale store. Residents in two apartments were evacuated and are receiving assistance from the American Red Cross. Byron Area Schools also canceled classes due to the fire.
Source: http://www.livingstondaily.com/article/20121002/NEWS01/210020309

46. *October 1, Santa Rosa Press Democrat* – (California) **Authorities investigate three Santa Rosa arson fires.** An arsonist hurling bottles of flaming liquid started three fires September 30 in Santa Rosa, California, two at downtown churches and one at a civil engineering firm, Santa Rosa police and fire officials said October 1. The fires caused minor or virtually no damage, said the Santa Rosa fire's senior fire inspector. "All three of these are connected. They are similar both in the devices and the scenario," he said. Santa Rosa police searched the area but did not locate any suspects. There were no signs of damage at the Episcopal Church of the Incarnation. At St. Rose Catholic Church, large black scorch marks marred half of the double doors at the west entrance. The fires were reported almost simultaneously.
Source:
http://www.pressdemocrat.com/article/20121001/ARTICLES/121009978?tc=ar

47. *October 1, Marin Independent Journal* – (California) **Unstable' man in custody after standoff with Palo Alto police.** A mentally unstable man was taken into custody October 1 at a Palo Alto, California condominium complex after an hours-long standoff with negotiators and a SWAT team, police said. Officers received a report of a man holding a knife to his throat claiming he wanted to hurt himself, a Palo Alto police spokeswoman said. Officers evacuated condos and other residences a witness said. Residents had to walk out and leave their cars behind because the road was closed off and filled with emergency vehicles. Officers found the man at a nearby residence and talked to him but he refused to come out, police said. Officers eventually talked the man out of the residence and took him into a psychiatric hold. The Santa Clara County Bomb Squad responded because the man had threatened to blow up the home. The bomb squad determined there was no hazard. The man could face charges for criminal

threats and making an incendiary device, police said. Some residents were allowed to return home several hours later.
Source: http://www.marinij.com/ci_21676270/suicidal-man-custody-after-standoff-palo-alto-police

For more stories, see items **31** and **34**

[Return to top]

National Monuments and Icons Sector

48. *October 2, Associated Press* – (Pennsylvania) **Deer poacher convicted of killing Pa. game warden.** A deer poacher was convicted of first-degree murder October 2, for the slaying of the Pennsylvania game warden near Gettysburg in November 2010. The jury delivered the verdict against the convicted man, and prosecutors intended to seek the death penalty. Investigators said the man and a friend had poached a deer at night when the game warden pulled them over on a dark stretch of rural road. The convict, though, was not allowed to have gun because he was a convicted felon. A passenger i the car testified that a shootout began after the convict vowed he would not go back to prison. Jurors were told the two men fired 25 shots in the exchange that left the game warden dead and the suspect injured.
Source: http://abcnews.go.com/US/wireStory/deer-poacher-convicted-killing-pa-game-warden-17375990#.UGsKm674LxN

[Return to top]

Dams Sector

49. *October 2, Associated Press* – (Louisiana) **Corps repairs damage from 2011 flooding.** The U.S. Army Corps of Engineers announced repairs October 1 to address damage from the 2011 historic Mississippi River flood. The work included $2.8 million in sheet piling work to deal with seepage on the Mississippi River levee near the Huey P. Long Bridge in Jefferson Parish and $1.9 million in sheet piling to deal with seepage in Algiers in New Orleans. In St. Mary Parish, the agency will spend $2 million to repair pump stations in Plattenville, and $2 million to reduce the risk of river flooding and prevent seepage under the Wax Lake east and west pumps stations. The Corps also will spend $2 million to repair pump stations in Franklin, Centerville, and Northbend.
Source: http://www.dailycomet.com/article/20121002/APN/1210020633?Title=Corps-repairs-damage-from-2011-flooding&tc=ar

[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 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