



Homeland Security

Daily Open Source Infrastructure Report for 18 October 2010

Current Nationwide Threat Level

ELEVATED



Significant Risk of Terrorist Attacks

For information, click here:
<http://www.dhs.gov>

Top Stories

- Reuters reports that a U.S. Senator said a planned New York-New Jersey Hudson River rail tunnel — whose future now is in jeopardy — is vital for the security of the surrounding area where 12 million people live. (See item [18](#))
- According to the Associated Press, West Virginia regulators plan to investigate a multiple-county phone outage, after it was informed by the Kanawha County Commission president that FiberNet did not notify Metro 911 or other agencies about the outage. (See item [48](#))

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

Current Electricity Sector Threat Alert Levels: **Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - <http://www.esisac.com>]

1. *October 15, Associated Press* – (Mississippi) **MS officials: Gas line explodes near Camp Shelby.** Workers have shut down a leaking natural gas line off U.S. Highway 49 near the Carnes community south of Hattiesburg, Mississippi. The pipe burst October 14. The chief of Carnes Volunteer Fire Department told the Hattiesburg American that no injuries were reported. Nine homes were evacuated overnight as a precaution, and Gulf South, the owner of the pipeline, shut down the line around 6 p.m. October 14.

Crews were scheduled to be back at the scene October 15. At least 20 firefighters were called to the scene of the leak.

Source: <http://www.wdam.com/Global/story.asp?S=13326019>

2. *October 14, Louisville Courier-Journal* – (National) **Obama administration unveils mining rules to curtail black lung disease.** The Presidential administration unveiled sharp new limits October 14 on miners' exposure to hazardous coal dust that is responsible for about 1,500 miners' deaths a year from black-lung disease. Federal regulators want to cut the dust exposure limit in half over 2 years, under rules proposed by the Mine Safety and Health Administration (MSHA). MSHA also would require mine operators for the first time to monitor and record dust levels in real time; require miners in the dustiest jobs to wear personal dust monitors; change sampling procedures to determine how well mines are complying with dust controls; and expand medical monitoring of miners. The changes are outlined in a proposed rule to be published October 19 in the Federal Register. The deadline for industry and public comments is February 28. Public hearings will be held on the new regulations, but times and places have not yet been set. They would affect about 72,000 miners working in more than 400 underground mines, and more than 1,100 surface mines.
Source: <http://www.courier-journal.com/article/20101014/NEWS01/310140040/Obama+administration+unveils+mining+rules+to+curtail+black+lung+disease>
3. *October 14, Reuters* – (National) **Government to conduct surprise oil rig inspections.** The U.S. offshore drilling agency will begin conducting surprise inspections on oil rigs as part of a new aggressive enforcement effort adopted by the Presidential administration since the BP oil spill, the agency's head said October 14. The Interior Department's Bureau of Ocean Energy Management, formerly known as the Minerals Management Service, had stopped performing unannounced rig inspections recently because of concerns about national security. But the head of the bureau said he saw no legitimate reason to let oil companies know about planned inspections as much as 2 days in advance. The department will provide companies some notice about inspections but not a full day ahead of the inspection. The bureau has also imposed stringent new safety rules aimed at preventing another drilling accident like the April 20 incident at BP's Macondo well that poured millions of barrels of oil into the Gulf of Mexico.
Source: <http://www.reuters.com/article/idUSTRE69D5YW20101014>
4. *October 14, WPTY 24 Memphis* – (Arkansas) **Swarms of earthquakes hit central Arkansas.** Central Arkansas has been hit by a series of earthquakes recently, the biggest being a magnitude 4.0 that shook the town of Guy, about 150 miles west of Memphis, Tennessee. A research scientist from the University of Memphis said Arkansas is getting many unusual earthquakes, more than 60 in the last month. "In the New Madrid Seismic Zone, there's approximately 200 per year, so if we had that many in Central Arkansas in less than a month, something is going on," the scientist said. That part of central Arkansas isn't even part of the New Madrid Fault Zone, so researchers are trying to determine what's causing the earthquakes. The scientist thinks

they may be the result of injecting salt water into old natural gas wells to force more gas production. Even though the two areas are not connected, his biggest worry is along the New Madrid fault where damage from a magnitude 6.0 earthquake could be catastrophic. “A probability of having that in a 50-year period is about 25 to 40-percent chance,” the scientist said. There have been no reports of damage or anyone getting hurt from the earthquakes.

Source: <http://www.myeyewitnessnews.com/news/local/story/Swarms-of-Earthquakes-Hit-Central-Arkansas/UpIqQoKMgEKYVpCn3JQ5qA.csp>

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

Chemical Industry Sector

5. *October 15, Scranton Times-Tribune* – (Pennsylvania) **State overseeing chemical spill cleanup efforts at Olyphant plant.** Cleanup of the October 13 chemical spill at an Olyphant, Pennsylvania manufacturing plant is under way, and state officials do not believe the spill will have a lasting impact on the environment. A faulty heater is being blamed for the spill that sickened more than two dozen people at Insituform Technologies, the plant manager confirmed October 14. The spill created a plume that spread across the region, sending plant employees, local police, and firefighters to hospitals for treatment of dizziness, nausea, and eye and throat irritation. State Department of Environmental Protection (DEP) officials were at the plant October 14 to oversee cleanup of the spill. A DEP spokesman said Insituform was required to hire a contractor to complete the cleanup. On October 13, plant officials said the chemicals were in the family of organic peroxide and that the reaction that formed the cloud did not pose a toxic threat to the public. According to Insituform’s main Web site, the company replaces, repairs and protects pipelines for sewers, drinking water, energy and mining, using technology that avoids the expense and disruption that can result from traditional dig-and-replace methods.

Source: <http://thetimes-tribune.com/news/state-overseeing-chemical-spill-cleanup-efforts-at-olyphant-plant-1.1049129>

6. *October 14, Ventura County Star* – (California) **People evacuated after chemical fire at Amgen facility.** A two-story building at the Amgen facility in Thousand Oaks, California, was evacuated October 14 following a chemical fire. Five units of the Ventura County Fire Department responded after a smoke alarm went off just before 2 p.m. in Building 29 on the Amgen campus, near the corner of Rancho Conejo Boulevard and Hillcrest Avenue. After fire investigators determined the fire was out, they identified the two chemicals involved as noncombustible sodium hydroxide, and lithium aluminum hydroxide, a flammable metal considered very corrosive to skin that reacts violently with water. “It’s actually fairly commonly used in laboratories,” said an Amgen corporate communications officer. Fourteen people who had minor exposure to the chemicals were medically evaluated on site. The communications officer said the cause of the minor spill will be investigated.

Source: <http://www.vcstar.com/news/2010/oct/14/chemical-fire-in-to-14-people-under-medical/>

7. *October 14, WHO DT 13 Des Moines* – (Illinois) **Chemical plant fire burns out after five days.** A chemical fire at the Euclid Chemical plant in Sheffield, Illinois burned out October 14 after smoldering for 5 days. The plant has been declared a total loss; firefighters attempted to fight the blaze and save the building the morning of October 9 but were pulled back after several reported having trouble breathing due to toxic chemicals. None of the plant's 15 employees were injured in the fire. Analysts from the federal Environmental Protection Agency will remain on site to monitor chemical levels. The cause of the fire has not been determined.
Source: <http://www.whotv.com/wgad-euclid-chemical-plant-fire-burned-out-101410,0,6466337.story>

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

Nuclear Reactors, Materials and Waste Sector

8. *October 15, Las Vegas Review-Journal* – (Nevada) **Yucca Mountain Project directive prompted rare NRC confrontation.** A directive for scientists at the Nuclear Regulatory Commission (NRC) to begin closing out their evaluation of the Yucca Mountain Project near Las Vegas, Nevada prompted a confrontation among the agency's leaders, according to officials and documents made public October 14. One of the five commissioners who head the independent nuclear safety agency protested in a private memo. On October 8, commissioners voted by written response. A NRC spokesman said the result effectively upheld shutdown guidance that had been issued through a budget memo signed off by the Chairman. After one commissioner raised the issue, he and another commissioner voted to allow staff to release a Yucca Mountain safety evaluation report. The remaining three "declined to participate in the matter," NRC sources said. In the absence of a quorum, the directive stood. "The commission did not change the existing approach as a result of this vote," the NRC's director of public affairs said. So the NRC "will proceed to an orderly closure of high level waste activities," as outlined in an announcement. A volume of the agency's safety evaluation report that was scheduled to be released next month will not be released, and staff will archive its work with \$10 million allocated for 2011, officials said.
Source: <http://www.lvrj.com/news/yucca-mountain-project-directive-prompted-rare-nrc-confrontation-104999364.html>

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

Critical Manufacturing Sector

9. *October 15, Reuters* – (National) **GM recalls Chevy Impalas on seat belt issue.** General Motors Co is recalling 322,409 model year 2009 and 2010 Chevrolet Impala sedans because front seat belts may not be properly anchored, the automaker and federal regulators said October 15. No injuries or fatalities have been reported in cases where the seat belts were not securely anchored or twisted, GM said in a letter to the U.S. National Highway Traffic Safety Administration (NHTSA). GM said it will begin asking its Impala customers later this month to bring the sedans to dealerships for

inspection and repair if necessary, free of charge. Through mid-August, GM told NHTSA it had received 32 warranty reports of seat belts having separated from their anchorage. The vehicles involved in the recall were assembled in Ontario, Canada from April 2008 to March 2010, GM said. NHTSA said of the 303,100 Impalas recalled in the United States, about two-thirds of them were 2009 models.

Source: <http://www.reuters.com/article/idUSTRE69E2S620101015>

10. *October 13, CBC News* – (International) **Mercury leaked into Columbia River by smelter.** Workers at a Teck Metals Ltd. smelter in Trail, British Columbia, Canada accidentally allowed up to 15 kilograms of mercury to leak into the Columbia River the week of October 4. Exactly how much mercury got into the river is still under investigation, but the company estimates it was between 12 to 15 kilograms — an amount that greatly exceeds what it is permitted to discharge. The mercury leaked from the company's massive lead-zinc smelter about 10 kilometers north of the U.S. border while workers were reconfiguring waste effluent piping, according to Teck's public affairs manager. British Columbia's ministry of environment is investigating the leak and will decide whether charges will be laid.

Source: <http://www.cbc.ca/canada/british-columbia/story/2010/10/13/bc-teck-smelter-mercury-dump.html>

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

Defense Industrial Base Sector

Nothing to report

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

Banking and Finance Sector

11. *October 15, Sun-Times Media Wire* – (Illinois) **Two women stole \$6M in mortgage scheme: Cops.** Two women have been charged with stealing more than \$6 million through a mortgage escrow scheme. The two suspects were charged in a 55-count indictment handed down by a DuPage County, Illinois grand jury October 12, a release from the DuPage County State's Attorney's office said. The fraud was allegedly run through PLM Title Co., which one suspect owned with the other suspect as a silent partner between November 2007 and April 2008, the release said. The indictment alleges the thefts took place during closings on new real estate purchases and refinancing transactions. According to the indictment, the new mortgage holder would wire money into a PLM Title escrow account, the release said. Instead of using the money to pay off the client's former mortgage holder, the suspects would use it for personal expenses or business operating costs, the indictment said.

Source: <http://www.myfoxchicago.com/dpp/news/metro/pamela-williams-patricia-johnson-6-million-mortgage-scheme-stolen-arrested-20101015>

12. *October 14, Associated Press* – (New York) **Police: NYC officer shot bank robber in Manhattan.** A knife-wielding robber targeted a bank in one of the busiest spots in Manhattan, New York October 14, his escape halted by a police officer's bullet that sent pedestrians ducking for cover, police and witnesses said. A uniformed police officer who happened to be in the area saw the man in his 60s fleeing from the Chase Bank branch located next to entrances to Madison Square Garden and Pennsylvania Station and shot him in the leg, police said. The shooting happened in front of an Amtrak loading dock, down the block from a heavily trafficked stretch of street. The suspect was taken to a hospital, where he was conscious and speaking to doctors, police said.

Source:

<http://www.google.com/hostednews/ap/article/ALeqM5iIwkO4ufq3VJ2Pn3j51meQiuHimwD9IRL5R80?docId=D9IRL5R80>

13. *October 14, ABC News* – (New York) **As terror alert continues, NYPD holds drill to prep for Mumbai style attack.** As U.S. officials proclaim an alleged European terror plot still active, New York City police conducted a drill October 14 that simulated a Mumbai, India-style attack on civilians on a crowded street in Manhattan's financial district. The drill simulated an attack near Wall Street and Ground Zero, on a mock block that contained a department store, a hotel, and a federal regulatory agency. The New York police commissioner addressed the media before the drill which began with two large explosions. "This is what we do," he explained. "We think the unthinkable." The drill simulated multiple bombs and shooters, including a bomb under a vehicle, and police responded with helicopters, dogs, automatic weapons, and an armored car. In the immediate aftermath of the 2008 Mumbai assault that claimed 175 lives, the New York Police Department (NYPD) revised its tactics to deal with a terrorist commando assault. During October 14's drill in the Bronx, heavily armed Emergency Service Unit officers were backed by officers from the Organized Crime Control Bureau (OCCB) trained to respond to such an attack. The OCCB officers are intended to beef up the NYPD response and prevent multiple simultaneous attacks from overwhelming the responding force.

Source: <http://abcnews.go.com/Blotter/terror-alert-continues-nypd-holds-drill-prep-mumbai/story?id=11879452>

14. *October 14, Gov Info Security* – (International) **Bugat is new malware of choice.** Last week's LinkedIn phishing attack did not deliver Zeus, the best-known and widely distributed Trojan, said malware researchers, but instead delivered its less well-known cousin, Bugat. This move is important said researchers who point to the emergence of Bugat as an attempt by cyber criminals to diversify attack tools, using a platform similar to Zeus, but harder to detect. While Zeus, Clampi and Gozi may be better known malware, Bugat's attack is similar, said a SecureWorks' technical director for malware analysis, Bugat can function as a SOCKS proxy server, upload files from the infected computer to a remote server, or download and execute programs. The Bugat Trojan communicates with a command and control server from where it receives instructions and updates to the list of financial Web sites it targets. This communication can be encrypted in order to thwart traffic inspection tools. Malware researchers at

Trusteer said the new version of the Bugat malware is used to commit online fraud. This version targets Internet Explorer and Firefox browsers and harvests information during online banking sessions. The stolen online banking credentials are used to commit fraudulent ACH and wire transfer transactions mostly against small to midsized businesses, which result in high-value losses. Bugat is three times more common in the United States than Europe, but its distribution is still fairly low.

Source: http://www.govinfosecurity.com/articles.php?art_id=3011

15. *October 14, IDG News Service* – (International) **Europe's ATM skimming attacks rise, but losses fall.** European banks reported a record number of skimming attacks, where payment card details were captured by criminals as bank customers tried to withdraw cash from ATMs. Banks reported 5,743 attacks in the first 6 months of 2010, according to the European ATM Security Team (EAST), a nonprofit group composed of national payment organizations, financial institutions, and law enforcement. The figure represents a record high since EAST first began keeping statistics in 2004. The number of attacks was 3 percent higher than the second half of 2009, and up 24 percent over the first half of 2009. But despite the higher number of attacks, losses fell. Skimming losses were \$202.1 million for the first half of this year, down 7 percent from the \$216.9 million reported in the last half of 2009. The decline is likely due to a few factors, said the EAST coordinator who prepared the report. Nearly 95 percent of cash machines in 31 countries in the Single European Payments Area (SEPA) are chip-and-PIN (Personal Identification Number) cards or EMV (Europay, MasterCard, Visa) cards. An EMV-compliant ATM will confirm the card's PIN via the microchip in order to let a transaction proceed. But most payment cards still have a magnetic stripe on the back containing the card's account details. That is the target of fraudsters. By attaching an external recording device near where a bank card is inserted into an ATM, a fraudster can "skim" those details and encode them onto a dummy or clone card.

Source:

[http://www.computerworld.com/s/article/9191120/Europe s ATM skimming attacks rise but losses fall](http://www.computerworld.com/s/article/9191120/Europe_s_ATM_skimming_attacks_rise_but_losses_fall)

16. *October 14, Minneapolis Star Tribune* – (Florida; Minnesota) **SEC sues Florida hedge fund managers in Ponzi scam.** On October 14, the Securities and Exchange Commission (SEC) charged two Florida-based hedge fund managers and their funds with defrauding investors out of \$1 billion, or nearly one-third of the total losses in the \$3.65 billion fraud that was carried out by another individual based in Minnesota. The two Palm Beach Capital Management and fund managers were accused by the SEC in a civil action of violating federal securities laws by misleading investors about the quality and status of their funds invested with the other alleged Ponzi scheme mastermind. The SEC complaint said the fund managers "pocketed" \$58 million in fees between 2004 and 2008 when they were making the investments. Investors with Palm Beach Capital Management and an affiliate fund were characterized by the SEC as individuals, foundations, family trusts, and other hedge funds from across the United States.

Source:

<http://www.startribune.com/business/104995449.html?elr=KArksLckD8EQDUoaEyqyP4O:DW3ckUiD3aPc: Yyc:aUvDEhiaE3miUsZ>

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

Transportation Sector

17. *October 15, Associated Press* – (New York) **Brooklyn Bridge reopened after false alarm.** The Brooklyn Bridge in New York City was reopened after police said a report of a suspicious package turned out to be a false alarm. The report came in at 9:38 a.m. October 15. The bridge was reopened less than 1 hour later. Police said someone on the walkway saw a flashlight with copper wiring and called 911. Pedestrian traffic was also briefly closed. The bridge, which was opened in 1883, is undergoing a series of renovations for the next several years. There is a lot of construction on both the Manhattan and Brooklyn sides of the bridge.
Source: <http://www.wcax.com/Global/story.asp?S=13329616>
18. *October 14, Reuters* – (New York; New Jersey) **Senator says new Hudson tunnel vital for security.** A planned New York-New Jersey Hudson River rail tunnel — whose future now is in jeopardy — is vital for the security of the surrounding area where 12 million people live, a U.S. Senator said October 14. After the deadly September 11, 2001, air attacks, “the only (mass) transportation that was really viable was rail,” the New Jersey Senator said at a news conference in Newark, New Jersey’s Pennsylvania Station. Amtrak, the national rail passenger service, kept running though airports were shut, he noted. “We have to have that available access to permit us to react in the event of an attack or a national disaster,” the Senator continued. The assessment by the Senator, who chairs a subcommittee on homeland security, raised the stakes for the Hudson River rail tunnel project midway through a 2-week review period of its \$8.7 billion budget. One day after the New Jersey governor canceled the project, saying New Jersey cannot afford an estimated \$2 billion to \$5 billion of extra costs, the Senator agreed to review the finances at the request of the U.S. Transportation Secretary. “I have not ruled it out; I have not ruled it in,” the Senator said, explaining that first the budget must be finalized.
Source: <http://www.reuters.com/article/idUSTRE69648520101015>
19. *October 14, KRTV 3 Great Falls* – (Montana) **Coal train derails in Great Falls, Montana.** A BNSF train went off the tracks near the Great Falls Police Department in Montana October 14. A total of 13 empty coal cars derailed around 3:30 a.m. There were no injuries and no hazards reported. The train was headed from British Columbia, Canada to Wyoming and was switching cars in Great Falls when it went off the tracks. The rail line, which runs five to seven trains, was opened up just before 3 p.m. October 14, and crews were able to pick up and move the derailed cars shortly after that. According to BNSF, the train was traveling at a speed of less than 2 miles per hour at the time of the derailment. The incident is still under investigation. A BNSF representative said there was minimal damage to both the rail cars and the track.
Source: <http://www.kx1h.com/news/coal-train-derails-in-great-falls/>

For more stories, see items [1](#) and [38](#)

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

Postal and Shipping Sector

Nothing to report

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

Agriculture and Food Sector

20. *October 15, Food Safety News* – (Ohio) **Eight Salmonella victims attended team dinner.** Salmonella sickened eight people who attended a function at Clearview High School in Lorain, Ohio, according to the Lorain County General Health District. A health commissioner said an Ohio Department of Health laboratory analysis confirmed that all were positive for Salmonella B. Meanwhile, local health investigators are trying to determine the source of the illness. He told the Morning Journal newspaper the investigation is focusing on a weekly football team dinner that all eight victims attended. The Chronicle-Telegram newspaper said at least two of the confirmed Salmonella cases were members of the football team. Those infected with Salmonella were among about 100 students reported to have been out sick during the first week in October, but the high rate of absenteeism at the high school likely was coincidental to the Salmonella outbreak, the health commissioner told the Morning Journal. He said the majority of ill students probably had upper-respiratory problems.
Source: <http://www.foodsafetynews.com/2010/10/ohio-salmonella-cases-linked-to-school-event/>

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

Water Sector

21. *October 15, Fort Myers News-Press* – (Florida) **Charlotte County employee accused of stealing copper from wastewater plant.** A wastewater treatment plant employee and two alleged accomplices were arrested October 14 on charges of stealing copper wire at the facility in Port Charlotte, Florida, according to the Charlotte County Sheriff's Office. Detectives began surveillance after receiving a tip. They followed a van and watched it drive down Old Landfill Road into the plant at 3100 Loveland Blvd. A sheriff's aviation helicopter was called, and using night-vision equipment, the van was located on the property that is secured by an electronic fence. Detectives found the van, three adults and an 8-year-old boy. They observed a ladder positioned under a power box with a large copper line cut and a rope tied around it. They found a pair of bolt cutters at another power box 100 feet away, as well as a canvas bag containing tools and beer. Through questioning, detectives learned the three men had planned the theft and a plant employee let the other two men into the secured property. Police also learned this marked the second time copper was stolen from the site. The stolen wire

was taken to Allied Recycling and sold for \$900. The three adults were transported to the Charlotte County Jail and all were charged with grand theft and contributing to the delinquency of a minor. Bond was set at \$3,500 each.

Source: [http://www.news-](http://www.news-press.com/article/20101015/CRIME/101015017/1075/Charlotte-County-employee-accused-of-stealing-copper-from-wastewater-plant)

[press.com/article/20101015/CRIME/101015017/1075/Charlotte-County-employee-accused-of-stealing-copper-from-wastewater-plant](http://www.news-press.com/article/20101015/CRIME/101015017/1075/Charlotte-County-employee-accused-of-stealing-copper-from-wastewater-plant)

22. *October 14, Canadian Press* – (International) **Chemicals survive waste treatment to be released into environment: study.** Chemicals in household drugs and cleaning products routinely survive waste treatment and are released into the environment, where little is known about their effects on land, water, and human health, according to a study funded by the Canadian government. “What are really needed are risk assessments,” said a research consultant who conducted the study for the Canadian Council of Ministers of the Environment. “The whole ecosystem needs to be assessed for the effects of the materials that are present.” He looked at treatment in 11 Canadian communities from coast to coast. He analyzed sludge entering the system and “biosolids” at the end that are often spread on fields or used in land reclamation. His study looked for 82 different chemicals, including bisphenol A, which was declared a toxic substance October 13. Two dozen of the compounds were still present in more than half the treated samples. Bisphenol A remained in 86 percent of treated samples at an average concentration of 325 parts per billion. Triclocarban, an antibacterial agent found in soap and disinfectant and known to cause hormone disruption in rats, was found in all treated samples. The mood-stabilizing drug Carbamazepine was also found in low levels in all samples. Antibiotics, anti-fungal agents, fragrance compounds, and painkillers survived treatment in more than two-thirds of samples. He said it is hard to say to if any chemicals reached dangerous levels. Safe levels have not been set for many of them.

Source: http://www.winnipegfreepress.com/life/sci_tech/chemicals-survive-waste-treatment-to-be-released-into-environment-study-104965919.html

23. *October 14, Somerset Messenger-Gazette* – (New Jersey) **Rags flushed down toilets may be cause of Raritan sanitary sewer pump failure.** A pair of sanitary sewer pumps near the entrance to Cardinal Woods Park at Cardinal Way in Raritan, New Jersey will likely need to be replaced after they were knocked out of service during heavy rain that fell October 11. “This was a flood event,” said a borough engineer speaking at the October 12 borough council meeting. “The electrical control panel was completely submerged.” Both pumps were clogged with rags. He also noted that a high volume of stormwater seemed to have infiltrated the sanitary lines, which are made from PVC piping. He suggested an investigation be conducted to determine where the stormwater was coming into the sanitary lines. The rags that clogged the pumps may have been flushed down the toilets of one or more homes in the area, he said. After an automatic warning alarm was triggered, workers from a company hired by the borough were called to the site to install a bypass around the pumping station. “The bypass is working,” the engineer said. He suggested the borough purchase replacement pumps that are less likely to clog. Officials suggested letters be mailed to residents describing the “do’s and don’t’s” of what should and should not be flushed down a toilet.

Source: [http://www.nj.com/messenger-gazette/index.ssf/2010/10/rags flushed down toilets may be cause of raritan sanitary sewer pump failure.html](http://www.nj.com/messenger-gazette/index.ssf/2010/10/rags_flushed_down_toilets_may_be_cause_of_raritan_sanitary_sewer_pump_failure.html)

24. *October 13, Gothenburg Times* – (Nebraska) **Study shows seepage into city sewer.** Solutions to Gothenburg, Nebraska's aging sewer and trouble spots are now on the table, but they come with a cost. Estimates show the price tag at a little more than \$1 million for an intermediate fix and \$1.8 million to repair the system for a longer period of time. At the October 5 meeting of the Gothenburg City Council, a city engineer presented highlights of a more than 1-year-long study of the sewer system. The bottom line, according to the engineer who is president of Miller and Associates Consulting Engineers of Kearney, is inflow and infiltration — especially during wet weather — allows rainwater and groundwater to enter the system. That can be blamed on a 50-year-old plus sewer system with a variety of performance and operational deficiencies, he said. He said action is needed to determine where inflow and infiltration occurs so the level at the city's wastewater treatment plant can be maintained. The plant treats and discharges wastewater into the Platte River. Wastewater plant records show water, sewer and wastewater flows generally increase from May through September, the engineer said, which indicate seepage into pipes. The majority of the wastewater collection system appears to have enough capacity to handle normal flows with the exception of major rain events.

Source:

http://www.gothenburgtimes.com/index.php?option=com_content&view=article&id=1867:study-shows-seepage-into-city-sewer&catid=8:featured-articles

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

Public Health and Healthcare Sector

25. *October 15, Reuters* – (National) **CareFusion recall classified as most serious type.** The Food and Drug Administration has classified CareFusion Corp's August recall of 17,000 Alaris medication pumps as a Class I recall, the most serious type, the company said October 15. A Class I recall is a situation in which there is a reasonable probability that the product will cause serious health consequences or death. CareFusion said it is working to correct the problem by updating hardware on the pumps, which are used to infuse medication into a patient's circulatory system, and has recorded a reserve in its fiscal fourth quarter to complete remediation. On August 24, CareFusion recalled the Alaris PC model 8015 manufactured or serviced between December 2008 and September 2009. It said the pump could experience intermittent communication errors under certain wireless network conditions, freezing the pump's screen and possibly delaying therapy. If the communication error occurs during infusion, infusion continues as originally programmed but cannot be modified. When this occurs, stopping infusion to make any modification or programming changes causes the pump to shut down, with a delay in therapy, which could lead to serious injury or death. Source: <http://www.reuters.com/article/idUSTRE69E2DQ20101015>

26. *October 14, Federal Computer Week* – (National) **DOD, VA consider more integration for EHR systems, VA official says.** The Defense (DOD) and Veterans Affairs (VA) departments are considering creating a joint electronic health record (EHR) system as one of many options for system modernization, a top VA official said October 14. A single integrated system “is an option that both agencies would consider, but it is not the only option,” said the VA’s assistant secretary for information and technology in a conference call with reporters. He said DOD and VA have been holding “a series of productive discussions” on how to proceed on modernization goals for DOD’s AHLTA and VA’s VistA EHR systems. DOD officials said they are developing a new record system, to be known as EHR Way Ahead, with a decision due next year. VA and DoD are also collaborating on several projects involving partial integration of their EHR systems. In Chicago, the Capt. James A. Lovell Federal Health Care Center opened October 1 and is preparing to begin operations November 30 with partially integrated IT systems from VA and the Navy.
Source: <http://fcw.com/articles/2010/10/14/dod-va-electronic-health-record-veterans.aspx>
27. *October 13, Reuters* – (National) **Some fever scanners work, U.S. study finds.** Two commercially available scanners meant for use in airports and other public facilities can reliably detect people with fevers, making them useful during disease outbreaks, researchers of the U.S. Centers for Disease Control and Prevention reported October 13. Researchers found that the scanners, which work at a distance of 3 to 6 feet, do a better job of detecting fevers than when people are simply asked if they feel feverish. They tested three systems in several emergency rooms and found they detected about 90 percent of fevers. That compared with 75 percent accuracy when people were asked if they felt like they had a fever. Airport fever scanners were used in some countries during last year’s pandemic of H1N1 swine flu, and the 2003 outbreak of Severe Acute Respiratory Syndrome, which killed about 800 people globally before it was contained.
Source:
<http://ca.reuters.com/article/technologyNews/idCATRE69C5PP20101013?pageNumber=2&virtualBrandChannel=0&sp=true>
28. *October 13, Spokane Spokesman-Review* – (Washington) **Bomb squad blows up suspicious bag at hospital.** A bomb squad blew up a suspicious bag left in an employee parking lot October 13 at Deaconess Medical Center in Spokane, Washington. The Spokane Explosive Device Unit detonated the bag at Fifth Avenue and Monroe Street to the west of the hospital. When an employee parked his car in the gravel employee lot, he noticed the bag next to a concrete barrier near the alley between Fourth and Fifth avenues. He immediately notified Deaconess security, who called the Spokane Police Department. Officers responded just after 8 a.m. and located the bag. A police spokeswoman said there was not a threat, but a suspicious bag, which could have simply been discarded or left behind. Police did not want to take chances because there were suspicious signs on the bag, which officers declined to specify, she said. The bomb squad about 10:30 a.m. deployed a robot to collect the bag for a safe disposal.

Source: <http://www.spokesman.com/stories/2010/oct/13/monroe-street-shut-down-police/>

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

Government Facilities Sector

29. *October 15, Brattleboro Reformer* – (Vermont) **Man threatens President Obama.** A 43-year-old Vermont man who threatened to kill the president via his Twitter account and blog will receive a mental health evaluation October 18. At a detention hearing October 14, the suspect, of Rockingham, was permitted temporary release to get an in-person mental health evaluation at the request of the defense. He was indicted and pleaded innocent on one count of knowingly threatening to kill the U.S. President, October 13, in U.S. District Court in Burlington. On August 21, the suspect allegedly sent numerous tweets via his Twitter account, SmellyOlTerriss, which included threats to the President's life. "I am dying inside. And I am plainly stating to you that I am going to kill the president." Throughout the day he seems to have a conversation with himself through his tweets to the White House. "When we kill presidents, what's it like? (Don't forget; still a question)," he tweeted.
Source: http://www.reformer.com/localnews/ci_16343686
30. *October 15, WJXX 25 Jacksonville* – (Florida) **UNF security breach affects more than 100,000 IDs.** It appears more than 100,000 could be affected by a security breach at the University of North Florida (UNF) in Jacksonville, Florida that involves Social Security numbers. In an e-mail sent to students, UNF said a file may have been accessed by someone outside the country. The file contained personal information of high school and college students, plus anyone else who had expressed interest in the university. UNF said it is notifying the 106,884 people who were affected. About half of them (52,853) had their names and Social Security numbers compromised, and the rest (54,031) had their names and dates of birth compromised, according to UNF. The breach happened sometime between September 24 and September 29. UNF said the computer involved has been isolated, and the university is working with the FBI to determine the cause and intent of the breach.
Source: <http://www.firstcoastnews.com/news/topstories/news-article.aspx?storyid=171731&catid=3>
31. *October 15, Minneapolis Star Tribune* – (Minnesota) **Chemical spill cancels classes at Edina High and middle school.** A chemical spill before classes started early October 15 at Edina High School in Edina, Minnesota forced students and staff members to leave the building, and classes were canceled for the day there, and at the adjacent middle school. There are no reports of anyone harmed. The spill also disrupted homecoming activities scheduled for October 15 and 16. A few students were in the high school, along with staff members, when it was evacuated and closed for the day. Classes for about 1,900 students begin at 8:30 a.m. at the school, which houses grades 10-12 and is south of Hwy. 62 between the Tracy and Gleason Avenue exits. The spill, reported to the principal's office by a custodian about 7:20 a.m., was in a first-floor

chemistry class, when a neutralization tank backed up because of a clogged line, an assistant fire chief said.

Source:

http://www.startribune.com/local/west/105024549.html?elr=KArksCiUBcy7hUiD3aPc:_Yyc:aUHDYAGEP7eyckcUs

32. *October 14, Fresno Bee* – (California) **Bomb threat empties Visalia courthouse.** A bomb threat early October 12 forced the evacuation of the Tulare County Courthouse in Visalia, California. Authorities learned of the bomb threat about 8:20 a.m., according to the sheriff's department. The building was emptied by about 10 a.m., and a bomb-sniffing police dog from the Farmersville Police Department was called in. No bomb was found and the courthouse reopened at 2 p.m.

Source: <http://www.fresnobee.com/2010/10/14/2117958/bomb-threat-clears-visalia-courthouse.html>

33. *October 14, Defense Systems* – (National) **Army Cyber Command stands guard over computer networks.** The Army launched the Army Cyber Command (ARCYBER), the service's component of the U.S. Cyber Command, this month, centralizing existing resources in the Army's efforts to protect its global computer networks. The new command brings a number of the Army's cyber resources under one roof. That will ensure that the service's policy, force structure, capabilities development, resources and personnel can securely and effectively work together in cyberspace at the tactical, strategic and national levels, said an Army spokesman. The new command, which incorporates Army organizations such as the Army Network Enterprise Technology Command/9th Signal Command and parts of the 1st Information Operations Command/Land, will be incorporated into ARCYBER. ARCYBER also will oversee the cyber operations of the Army Intelligence and Security Command. ARCYBER's personnel level will exceed 21,000 soldiers and civilians. The new command gives the Army an organization that can plan, coordinate, integrate, synchronize, and conduct cyberspace operations.

Source: <http://defensesystems.com/articles/2010/10/15/cyber-defense-army-cyber-command.aspx?admgarea=DS>

34. *October 13, DarkReading, InformationWeek* – (International) **DARPA project to tackle inside security threats.** The technology research arm of the Department of Defense (DOD) plans to develop technology to determine ahead of time when soldiers or other government insiders may become a threat to themselves or others. The Defense Advanced Research Projects Agency (DARPA) is seeking ideas for its Anomaly Detection at Multiple Scales (ADAMS) program, which will produce technology that can sift through the behavioral signs that may lead to someone turning on his or her cohorts, and prevent the action before it happens, the agency said. "Each time we see an incident like a soldier in good mental health becoming homicidal or suicidal or an innocent insider becoming malicious, we wonder why we didn't see it coming," according to an announcement about an ADAMS industry day October 19. With ADAMS, the agency aims to "create, adapt, and apply technology to the problem of anomaly characterization and detection in massive data sets," according to DARPA.

Following the industry day, it will release a broad agency announcement on FedBizOpps.gov seeking proposals. DARPA hopes the military and the counterintelligence community can use the technology to catch potentially threatening behaviors “before or shortly after they turn,” it said. The agency defines an insider threat as one from a person already trusted in a secure environment who has access to sensitive information, systems, and sources.

Source:

<http://www.darkreading.com/security/government/showArticle.jhtml?articleID=227701306>

35. *October 13, Associated Press* – (Texas) **911 tapes and video released from UT shooting.** The University of Texas (UT) October 13 released audio and video recordings of the chaos that unfolded after a student opened fire on campus in September before eventually turning the gun on himself. “Get out of there!” one policeman yelled as students are seen fleeing the building where authorities said the 19-year-old ended his own life. The camera was flashing 8:21 a.m. when an unidentified man yells out: “He shot himself.” Meanwhile, in one of more than a dozen 911 calls released October 13, a UT project manager reported seeing the shooter walking down the street carrying an AK-47. The recordings, including police dashcam video and surveillance video, were released about 2 weeks after the shooter terrorized the UT campus. The shooting September 28 began near a fountain in front of the UT Tower — the site of one of the nation’s deadliest shooting rampages more than four decades ago, when a gunman ascended the clock tower and fired down on dozens of people.

Source: <http://www.chron.com/dispatch/story.mpl/ap/nation/7245742.html>

36. *October 13, KFVS 12 Cape Girardeau* – (Missouri) **Students could face charges in threats to school.** An adult and a juvenile student were expected to face charges as early as October 14 for making threats to the campus of Poplar Bluff High School in Poplar Bluff, Missouri. “Monday afternoon I get a call from my high school principal that we had a student write something on a bathroom stall,” the superintendent said. “The message was there will be a threat a bomb threat.” That was the first of two threats. The superintendent said leads directed them to a student who was removed from campus, and extra police were brought in. Then October 12, it happened again. Again, the student, this time a juvenile, was removed from campus and police stepped up security. Both threats turned out to be bogus.

Source: <http://www.kfvs12.com/Global/story.asp?S=13320077>

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

Emergency Services Sector

37. *October 14, New York City Comptroller’s Office* – (New York) **Audit: FDNY lab unit failed to monitor storage of hazardous materials.** Serious deficiencies at the New York City Fire Department (FDNY) unit charged with inspecting hazardous materials could result in potentially dangerous consequences for the public, as well as firefighters, according to an audit released by the New York City Comptroller October

14. The audit uncovered problems in the Lab Inspection Unit (LIU), a part of the FDNY's Bureau of Fire Prevention. The unit is responsible for inspecting locations that store hazardous materials including flammable liquids and solids, corrosive acids, and compressed gases. The locations include high schools, colleges, hospitals, nursing homes, manufacturing facilities, and factories. The audit looked at the FDNY's controls over the LIU's inspections from July 2006 through May 2010. FDNY agreed with all 15 recommendations, and has already begun taking steps to implement them to improve operations. Chief among the findings, lab supervisors conducted zero of the 20 required supervisory inspections during Fiscal Year 2009, and the FDNY did not inquire as to why these inspections were not performed.

Source: http://www.comptroller.nyc.gov/press/2010_releases/pr10-10-095.shtm

38. *October 14, Associated Press* – (Pennsylvania) **Police probe laser pointed at Pa. medical chopper.** Township police in western Pennsylvania are trying to find someone who shined a green laser into the cockpit of a Pittsburgh-area medical helicopter. A Stat MedEvac spokesman said the incident happened about 1:40 a.m. October 14, over North Huntingdon Township, about 25 miles east of Pittsburgh. The helicopter was heading back to its base in Greensburg after flying a patient to Pittsburgh. The main concern is the lights could distract pilots or their crew. The helicopter's base called 911 while the chopper shined a light on the ground while township police unsuccessfully searched for a suspect. The Federal Aviation Administration is still investigating two similar incidents involving Stat MedEvac helicopters in August. Using a laser to interfere with an aircraft is a federal crime.

Source: http://www.ldnews.com/news/ci_16347212

39. *October 14, Associated Press* – (Virginia) **Body of missing Coast Guard member recovered in Va.** The remains of the missing Coast Guard member who fell off a small boat during a training mission near the Monitor-Merrimac Bridge Tunnel in Hampton, Virginia have been found. The Coast Guard says crews recovered the body at about 5 p.m. Thursday, October 14. The member of the Maritime Safety and Security Team New York fell into the water at about 9:15 p.m. October 13. The accident occurred during tactical operations with the Coast Guard cutter. The search was being conducted by the Coast Guard, the Virginia Marine Police, and fire and police boat crews.

Source: <http://www.wcax.com/Global/story.asp?S=13326673>

For another story, see item [51](#)

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

Information Technology Sector

40. *October 15, The Register* – (International) **Anonymous plants pirate flag on MPAA Web site.** Hacktivists used DNS cache poisoning to deface a Motion Picture Association of America (MPAA) Web site, according to security analysts. The attack on copyprotected.com — a MPAA Web site that reports violations of the copy protection controls on DVDs and Blu-ray discs — is the latest in a string of assaults

against the entertainment business organized by the loosely affiliated Anonymous groups. The defaced page carried the logo of the Pirate Bay after the site itself was the victim of a DNS cache poisoning attack. “Someone managed to hijack the DNS registration for copyprotected.com such that it points to an IP with their own web server displaying their own page,” said a security researcher. The server displaying the defacement is run by WareNet. It seems the organization was unwittingly roped into the attack and might itself have been a victim. “I wonder if the Anonymous folks are DDoS’ing WareNet to keep them distracted while they’re quietly using a server in WareNet’s second IP block for their own purposes,” the researcher added.

Source: http://www.theregister.co.uk/2010/10/15/mpaa_site_dns_hack/

41. *October 15, Softpedia* – (International) **Serious vulnerability fixed in Ruby on Rails.** The Ruby on Rails development team has released security updates for the Web application framework, which address a serious vulnerability facilitating unauthorized record manipulation. The issue stems from the way nested attributes were handled in the latest Ruby on Rails versions, 3.0.0 and 2.3.9. “An attacker could manipulate form parameters and make changes to records other than those the developer intended,” the official advisory explains. The vulnerability is identified as CVE-2010-3933 in the Common Vulnerabilities and Exposures database. Older versions of the framework are not affected because the bug was accidentally introduced in version 2.3.9. It is also present in the first stable release from the 3.0.x series, 3.0.0, which was launched at the end of August.

Source: <http://news.softpedia.com/news/Serious-Vulnerability-Fixed-in-Ruby-On-Rails-161227.shtml>

42. *October 15, IDG News Service* – (International) **Google adds phishing alerts to network services.** Google said October 14 it has added notification of phishing URLs to the e-mail warnings it sends to administrators. Despite advances in detecting the sites, there usually is a short window of time the site is active before it is either blacklisted or shut down. Google’s Chrome browser has the “safe browsing” technology built in, which will block users from going to potentially harmful Web sites on the blacklist. The notification can also be sent in an XML data format, which allows administrators to process the notification using scripts to automate other functions, wrote a Google security team member.

Source:

http://www.computerworld.com/s/article/9191338/Google_adds_phishing_alerts_to_network_services

43. *October 15, Softpedia* – (International) **Facebook sued for exposing people’s names to advertisers.** According to a complaint filed by two Facebook users in California Northern District Court, the company knowingly violated its privacy policy by sharing personally-identifiable information with advertisers. From February 2010, following a Web site update, Facebook began including user IDs and/or usernames in Referer headers, therefore allowing advertisers to identify people who clicked on their ads. Both the user ID and username can be used to access a person’s Facebook profile, which contains their name. Knowing these identifiers, advertising companies can build

automated scripts to associate people with ad clicks.

Source: <http://news.softpedia.com/news/Facebook-Sued-for-Exposing-People-s-Names-to-Advertisers-161101.shtml>

44. *October 14, Softpedia* – (International) **Avira temporarily blocks Google, CNN and others.** On October 14, Avira users were unable to access Google, CNN, and other popular Web sites, because of bogus detections triggered by the WebGuard component. “For a short time this morning (between 7a.m. and 8:45 a.m. MEST), some domains slipped through into our WebGuard filtering system which caused some users to not be able to visit some regular web sites,” the German antivirus vendor announced on its blog. Apparently, the links were improperly detected as phishing URLs by new filters introduced as a result of a recent spam campaign, which employed special techniques. The junk e-mails used HTML-based tricks to advertise rogue online pharmacies. They also included hidden links for several major Web sites like Google, Yahoo!, Amazon, or AOL, in an attempt to evade spam filters.

Source: <http://news.softpedia.com/news/Avira-Temporarily-Blocks-Google-CNN-and-Others-161058.shtml>

45. *October 14, The New New Internet* – (International) **Stuxnet spreads to Finland.** Corporate espionage is spreading in Finland, and the country was recently targeted by the infamous Stuxnet worm, Finnish newspaper Helsingin Sanomat reports. The complex malware has been found in at least one institution that uses the industrial equipment targeted by the worm. It has not caused any damage. In addition, Finnish state institutions have also been attacked. According to the Finnish Security Police, spyware has been spreading both through e-mail and via USB flash drives.

Source: <http://www.thenewnewinternet.com/2010/10/14/stuxnet-spreads-to-scandinavia/>

For more stories, see items [14](#) and [50](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <https://www.it-isac.org>

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

Communications Sector

46. *October 15, SPAMfighter* – (National) **Security experts fear attack of Comcast botnet notification system.** Security experts fear that U.S. Internet Service Provider (ISP), Comcast’s latest botnet notification system will be abused by hackers. Details show in the last few months, Comcast will roll out service called “Constant Guard” to all 16 million subscribers. Customers will receive information about the working of

Botnet Identification and Notification service, and data on how hackers circulate malware through e-mails with harmful attachments, and Web links that make botnets out of many infected systems. The botnets are then controlled to circulate spam or initiate distributed denial-of-service attacks made to hit Web sites. Comcast's plan is being rejected by security experts as they foresee it as an exciting opportunity for forged AV/scareware hackers. A senior security advisor at Sophos cautions that these banners get injected into sites and spam customers with the messages leading them to standard fake AV installers. And customers who get a notice but are using a wireless router behind their cable modem, will not be able to figure out which system is infected with malware. The security experts suggested that ISPs who find infected machines on their networks disconnect the customer's Internet access until the infection is cleaned up properly. This would reduce botnet traffic tremendously and could make users more aware of good security practices. Also, the disconnection of Internet would immediately capture the user's attention.

Source: <http://www.spamfighter.com/News-15219-Security-Experts-Fear-Attack-of-Comcast-Botnet-Notification-System.htm>

47. *October 14, PC Advisor UK* – (International) **Half of home Wi-Fi networks vulnerable to hacking.** Nearly half of all home Wi-Fi networks in the U.K. could be hacked within 5 seconds, according to CPP. The life assistance company employed the services of an ethical hacker to roam six major cities and use specially developed software to identify home networks that were at risk of “Wi-Fi jacking.” Wi-Fi jacking involves hackers piggybacking on a net connection, which allows them to illegally download files, purchase illegal goods or pornography, or even sell stolen goods, without being traced. It also permits them to view the private transactions made over the Internet, providing them with access to passwords and usernames that can subsequently be used to commit identity fraud. CPP's research revealed 40,000 home Wi-Fi networks were at risk. CPP also said that despite the fact 82 percent of Web users believe their Wi-Fi connection is secure, nearly a quarter of private wireless networks are not password protected. Furthermore, nearly one in five Web users said they regularly use public networks. During his research, the hacker was able to “harvest” usernames and passwords from users of the public Wi-Fi networks at a rate of more than 350 an hour. He also revealed more than 200 web users unsuspectingly logged onto a fake Wi-Fi network over the course of an hour during the experiment, putting themselves at risk from fraudsters who could harvest their personal and financial information.

Source: <http://www.networkworld.com/news/2010/101410-half-of-home-wi-fi-networks.html?hpg1=bn>

48. *October 14, Associated Press* – (West Virginia) **State regulators to investigate recent FiberNet outage.** State regulators plan to investigate a recent FiberNet phone outage that affected several West Virginia counties. The Kanawha County Commission requested the investigation in a letter sent October 11 to the Public Service Commission (PSC). In the letter, the county commission president said FiberNet did not notify Metro 911 or other agencies about the October 10 outage. He said a general review is needed of all telephone landline providers' notifications to public safety agencies

during significant outages. The PSC said in an order issued October 13 that it will investigate the matters set forth in the county's letter. FiberNet issued an apology to customers October 11.

Source:

http://www.wsaz.com/huntington/headlines/BREAKING_NEWS_911_Down_in_Kanawha_County_104677564.html

49. *October 13, WLS 7 Chicago* – (National) **FBI agent warns of Wi-Fi cyber-theft.** For the first time in Internet history, free Wi-Fi hot spots in the United States outnumber the sites where people have to pay for access. The FBI is warning this may be actually be bad news for computer users. The latest market research reveals there are more than 71,000 wireless hotspots in the United States, a list that is growing each day. Chicago has almost 800 sites, just behind New York and San Francisco. The FBI's top cyber-security agent in Chicago warns that when one connects at the corner coffee shop, electronic thieves may be lurking. "Using coffee shop wireless or free Wi-Fi or especially hotel Internet is not safe," said a Special Agent of the FBI cyber-security unit. "You shouldn't be checking your personal emails and you definitely shouldn't be checking your personal bank accounts. Unless you are going to go ahead and change an email password as soon as you return home. They're unsecure. A lot of people just sit on them and they collect information and they're just looking for you to log into your bank account or they're looking for you to log into your emails and they're going to look through there to see if there is anything that can be used against you," he said.

Source: <http://abclocal.go.com/wls/story?section=news/iteam&id=7723367>

50. *October 11, SPAMfighter* – (International) **U.K. domain registrar targeted by mass injection attack.** Security firm Sucuri (a provider of Web integrity monitoring solutions and an operator of a Web site malware scanner) has reported a new mass injection attack that infected many Web sites harbored at 123-reg.co.uk, one of the biggest domain providers in the U.K. Malicious code embedded in these sites directs visitors to scareware. In the past few days, Sucuri has found many sites compromised with the same code used to inject malicious java script on many sites harbored at Go Daddy. All of them include a java script loading malware (the famous fake AV). The attack redirects users of the compromised Web sites to a scareware page that impersonates an anti-virus scan and displays fake alerts regarding malware infections on their machines. The objective of this trick is to scam users into downloading and installing a rouge anti-virus program that further attacks users' machine with several fake alerts and warnings to persuade them to buy a license. Users who purchase the license will not only pay a great amount for a worthless application, but will also compromise their credit card details in the procedure. Remarkably, the domain meqashopperinfo.com is not blacklisted. Hence, it has the ability to infect a very large number of computers, particularly the ones with outmoded AV signatures and definitions.

Source: <http://www.spamfighter.com/News-15182-UK-Domain-Registrar-Targeted-by-Mass-Injection-Attack.htm>

Commercial Facilities Sector

51. *October 15, St. Petersburg Times* – (Florida) **Bomb squad detonates empty briefcase outside Sears store in Brooksville.** A briefcase left outside a Sears store on Cortez Boulevard in Brooksville, Florida, October 14 prompted deputies to close off an area around the busy shopping center while a bomb squad detonated the suspicious package. After the blast, investigators discovered that the briefcase was empty. According to the Hernando County Sheriff's Office, a customer told a Sears manager around noon that there was a briefcase outside and that it could possibly have a bomb inside. The manager contacted authorities, who helped evacuate the store and then asked for assistance from the Tampa Bomb Squad. A Sears employee told deputies she had noticed the same briefcase outside the store October 12, but did not report it. Deputies reviewed store surveillance video from October 12 that showed a man walking in front of Sears while pulling a suitcase on wheels in one hand, and carrying the same briefcase in the other hand. The man sat down and took everything out of the briefcase and put it all into the suitcase before putting the briefcase on top of a nearby trash can and then walking away.
Source: <http://www.tampabay.com/news/publicsafety/crime/article1128149.ece>
52. *October 15, WHNS 21 Greenville* – (Florida) **Central police have person of interest in bomb blast.** Central, South Carolina police said they have a person of interest in connection with a bomb that exploded under a car at an apartment complex. Residents of the Summit at Cross Creek Apartments said the blast rattled windows October 14. A resident said he was in his kitchen when the device detonated. "It was basically like a shotgun that went off," he said. "I heard this loud explosion and it sort of rumbled." Investigators said someone planted a bomb near the back tire of a 2007 Honda Civic. They said the blast blew off the bumper and scattered debris throughout the parking lot. "We heard it all the way up here," said the Central police chief. The Central Police Department is about 500 feet away from the apartments where the explosion happened. The chief said moments after the blast, dozens of 911 calls were made. He also said what is left of the explosive device is now being analyzed in an effort to determine what kind of bomb it was.
Source: <http://www.foxcarolina.com/news/25397702/detail.html>
53. *October 14, WVIT 30 Hartford* – (Connecticut) **Residents allowed back after chemical spill in Middletown.** About 150 to 200 people had to evacuate the Wilcox Apartments at 309 South Main St. in Middletown, Connecticut after a chemical caused a vapor cloud outside the building October 14. As residents left the building, the fire alarm and sprinklers began to go off. Residents were worried about their possessions, but fire officials said, the water from the sprinklers was contained to the sprinkler room. The tenants were kept out of the building for about 9 hours and stayed at Woodrow Wilson Middle School. Crews responded after the complex hired people to clean debris on the property and they found a large bucket filled with clear liquid, tried to retrieve it and the bucket broke, officials from the state Department of Environmental Protection (DEP) said. Some of the liquid spilled into a brook, which leads to a pond, and it reacted with water, causing the cloud. Three employees were

taken to a hospital for an evaluation. DEP and fire departments are investigating what happened, and DEP will send a chemical sample to a lab for testing. Tenants were allowed back into the Wilcox Apartments around 8:30 p.m.

Source: <http://www.nbcconnecticut.com/news/local-beat/Hazmat-Situation-in-Middletown-Report-104961054.html>

For another story, see item [13](#)

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

National Monuments and Icons Sector

54. *October 15, Associated Press* – (Ohio) **Reward set in fire at Ohio historic flea market.** One of the owners of a historic Ohio flea market that has burned to the ground said many irreplaceable antiques were lost. She and her husband are offering a \$5,000 reward for the capture of the person who set the fire October 13 at the couple's Garver Flea Market in Strasburg. The state fire marshal said the blaze was among a rash of fires set deliberately within a relatively short time in an area about 60 miles south of Cleveland. No injuries were reported. The flea market was in a building on the National Register of Historic places that once housed a family business known as the "World's Largest Country Store."

Source: <http://www.wfmj.com/Global/story.asp?S=13328988>

55. *October 14, Salinas Californian* – (California) **Monterey County Sheriff's: 4,000 marijuana plants destroyed.** More than 4,000 marijuana plants were eradicated in the area of Fremont Peak State Park, the Monterey County Sheriff's Office in California announced October 14. The plants were found around 8 a.m. October 14, officials said, by members of the county's Marijuana Eradication Team, or COMMET, the sheriff's office narcotics unit, and an air unit from the California Highway Patrol. No suspects were found in the garden.

Source:

<http://www.thecalifornian.com/article/20101014/NEWS01/101014035/1002/NEWS01/4+000+marijuana+plants+destroyed+at+state+park>

56. *October 14, Victorville Daily Press* – (California) **Teen arrested in 66-acre wildfire.** A 17-year-old Crestline boy was arrested for starting a fire that burned 66 acres last August near Miller Canyon and the adjacent San Bernardino National Forest in California, officials said October 14. The Silverwood Lake State Recreation Area sustained some fire damage to the campground, however, there was no structure loss and no reported injuries, according to a San Bernardino County Sheriff's press release. A joint investigation by the sheriff's department and CAL FIRE identified a juvenile suspect. He was arrested and released to his parent with criminal charges pending.

Source: <http://www.vvdailypress.com/news/silverwood-22371-teen-wildfire.html>

For another story, see item [57](#)

Dams Sector

57. *October 15, BBC News* – (Arizona; Nevada) **Dedication of new Hoover Dam bridge.** A dedication ceremony has taken place for the Hoover Dam bridge, which has been completed after 8 years' work. The 1,900-foot structure high above the Colorado River allows travelers to bypass the Nevada dam much more quickly and with no checkpoints. The new four-lane bridge officially opens next week.
Source: <http://www.bbc.co.uk/news/world-us-canada-11550522>
58. *October 14, Morgan Hill Times* – (California) **Water district: Dam repairs needed.** If Anderson Dam in Santa Clara, California, were to fail in the event of a large earthquake — less than a 1 percent chance - the drinking water behind it could flood downtown Morgan Hill to a depth of 35 feet. That is why the Santa Clara Valley Water District announced the week of October 11 the preliminary results of a study of the dam's integrity indicate a retrofit costing up to \$100 million is needed. "Based on other dams that have had similar issues, it could cost tens of millions to a hundred million dollars," the district's deputy operating officer said. The study by Oakland-based AMEC Geomatrix found that "significant slumping" could occur if a 7.25-magnitude earthquake or larger occurred on the Calaveras fault, within 2 kilometers of Anderson Dam, according to a statement from the water district. The lower, inside portion of the dam contains loosely compacted dirt-like material that could liquefy in the scenario that such extreme earth-shaking happened. In that event, the shell on the upstream and downstream sides of the dam could slide downhill, causing the water in Anderson Lake to spill over the slumping dam. "The rock shells would slip and move downhill to some degree. 'Significant' means it's not a foot or two - it's more like 10 [feet] or more," he said. A retrofit would likely entail a combination of two options — replacing the loosely packed materials inside the dam, and reinforcing both sides with more rocks. The final study is not expected to be complete until May 2011. The water district provides wholesale drinking water and flood protection for 1.8 million residents of Santa Clara County.
Source: <http://www.morganhilltimes.com/news/269532-water-district-dam-repairs-needed>
59. *October 13, Charleston Gazette* – (West Virginia) **Acid mine drainage kills fish in Kanawha creek.** A spill of iron-laden, acidic mine drainage has caused a fish kill along 9 miles of Blue Creek, a bass and trout stream in eastern Kanawha County, West Virginia. The spill, which began October 2 or 3 in a small headwater tributary known as Morris Fork, killed fish in Blue Creek all the way down to the town of Coco. A district fisheries biologist for the state division of natural resources, said a state-government attempt to clean up an abandoned mine actually caused the spill. "There is a mine up on the ridge between Blue Creek and Campbells Creek that had been discharging water for some time," he said. "Supposedly the [state Department of Environmental Protection] had a contractor doing some abandoned-mine cleanup work there. As I understand it, the workers were trying to do away with the old impoundment

the mine discharged water into. When they opened the impoundment up, they got more water than they expected,” the biologist said. “At first the water wasn’t acidic, but the more water flowed out the more acidic it became.” He said the water flowed for a week before it started producing acid and iron and started killing fish. “The fish kills started happening on October 3. The bottom line is that we’ve lost about 9 miles of a pretty high-quality stream,” he said. “After the DEP folks get the acid problem solved, it will probably take 2 to 3 years for the stream to bounce back.”

Source: <http://sundaygazettemail.com/News/201010131020>

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

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/iaipdailyreport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at 703-872-2267

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@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.