



# Homeland Security

Daily Open Source Infrastructure Report  
6 October 2011

## Top Stories

- The Veterans Affairs department may have issued more than 157,000 identification credentials without authenticating the identity of the individuals who received them, a new report found. – *Federal Computer Week* (See item [28](#))
- Authorities were searching door to door the afternoon of October 5 in a neighborhood about 5 miles from a Cupertino, California quarry where a gunman killed two and wounded six that morning. – *msnbc.com*; *Associated Press* (See item [44](#))

---

## 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: LOW, Cyber: LOW**

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

1. *October 4, Reuters* – (Maryland; National) **U.S. alleges \$9 million biofuel scheme paid for exotic cars.** A Maryland man has been charged by the federal government for selling \$9 million in fraudulent renewable fuel credits and using the money to buy a Ferrari, a Lamborghini, and a Maserati, among other things. The U.S. Environmental Protection Agency (EPA) said October 4 the owner of Clean Green Fuel, LLC, was charged with wire fraud, money laundering, and violation of the Clean Air Act in connection to trade in renewable identification numbers (RIN) purportedly produced by

his company. The government alleges that between March 2009 and December 2010, the man sold more than 32 million RINs to brokers and oil companies for at least \$9 million. But the government claims Clean Green Fuel had produced no fuel at all. “According to the criminal information, [the man] did not have a facility capable of producing biodiesel fuel and his business operation consisted solely of generating false RINs on his computer and marketing them to brokers and oil companies,” the EPA said in a release. To encourage renewable fuel output, the government requires oil companies that market petroleum in the United States to produce a given quantity of renewable fuel, or to purchase the RIN credits from producers of renewable fuels. During an investigation, the man made numerous false statements to EPA investigators, including that he manufactured the fuel from waste vegetable oil collected from 2,700 restaurants, it said. The man had registered the company with the EPA as a producer of biodiesel.

Source: <http://www.reuters.com/article/2011/10/04/us-usa-ethanol-fraud-idUSTRE7935AU20111004>

2. *October 4, Tahlequah Daily Press* – (Oklahoma) **Two die in tanker crash.** Two people were killed October 3 in a crash between a passenger car and a tanker truck loaded with diesel fuel in Tahlequah, Oklahoma. Tahlequah police, Tahlequah-Cherokee County Emergency Management, and other agencies were still at the Grand Avenue-Bertha Parker bypass intersection late October 3 working on clean up of several thousand gallons of fuel. The crash occurred shortly before 6 p.m. Both of the fatalities were in the passenger car, and the driver of the tanker truck was reportedly flown to a Tulsa hospital. Both vehicles ended up on the east side of the bypass. Personnel from Eagle Med, Tahlequah City Hospital EMS, Cherokee Nation EMS, Tahlequah firefighters, a hazardous materials unit from Tahlequah-Cherokee County EM, Tahlequah police, Cherokee County sheriff’s deputies, and Cherokee Nation marshals responded.

Source: <http://tahlequahdailynews.com/local/x1953752312/Two-die-in-tanker-crash>

3. *October 4, Syracuse Post-Standard* – (New York) **Copper thieves target power company in Central New York.** National Grid is pushing back against copper thieves, who have targeted 24 electric substations in Onondaga County, New York, since the beginning of the year, the Syracuse Post-Standard reported October 4. In the last month, Onondaga County sheriff’s deputies have investigated 20 reports of copper thefts at National Grid substations and other facilities, the sheriff said. Syracuse police are investigating at least 15 cases, the police chief said. Recently, thieves stole \$800 in scrap metal and caused \$10,000 in damage at the Glenwood and Peat Street substations in Syracuse. The two substations have been hit at least three times apiece. In another case, someone was charged with stealing less than \$200 in copper from 35 utility poles near Syracuse University. The repairs cost \$14,000 — or \$400 a pole. A theft in southern Onondaga County required a 6-hour planned outage September 11 to fix. The price of copper — between \$3 and \$4 a pound — has led to “skyrocketing” copper thefts in the past year, authorities said.

Source:

[http://www.syracuse.com/news/index.ssf/2011/10/copper\\_thieves\\_target\\_power\\_co.html](http://www.syracuse.com/news/index.ssf/2011/10/copper_thieves_target_power_co.html)

For another story, see item [5](#)

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

## Chemical Industry Sector

4. *October 5, San Antonio Express-News* – (Texas) **Fire hits chemical plant again.** For the second time in 9 days, a fire was reported at a chemical plant in Atascosa County, Texas, prompting precautionary evacuations October 4. The fire at the Chemplex chemical facility on County Road 430 near County Road 422 was reported around 3:30 a.m. Officials ordered residents within 1 mile of the plant to evacuate, and firefighters and law enforcement officers went door to door to notify them. The same residents were evacuated September 26 after a small fire at the same plant. By 6 a.m., the fire had been extinguished, residents were able to return, and firefighters were being decontaminated, officials said. County Road 430 remained closed near the plant. Both fires started on wooden pallets inside the facility's gates, but the county fire marshal said the causes were still under investigation. "Two fires within (the short time period) — it's not normal." He said he wanted to craft evacuation procedures in case a similar situation occurs again. "We're going to get a satellite photo of the facility and homes and have lists of telephone numbers so we can call next time," the fire marshal said. Source: [http://www.mysanantonio.com/news/local\\_news/article/Fire-hits-chemical-plant-again-2201595.php](http://www.mysanantonio.com/news/local_news/article/Fire-hits-chemical-plant-again-2201595.php)
5. *October 5, KXAS 5 Dallas-Fort Worth* – (Texas) **Water runoff biggest problem after chemical fire.** More than 24 hours after igniting, the fire at the Magnablend Inc. plant in Waxahachie, Texas, was still smoldering late October 4. While the smoke has a foul odor, continued U.S. Environmental Protection Agency (EPA) air quality tests show it does not pose a public health threat. But the runoff from the water firefighters used to douse the blaze that began October 3 is a concern. The water is in ditches near the site. The Waxahachie fire chief said public works crews brought in sand and back hoes to dam up the water. Magnablend's owner said oil and gas products comprise 80 percent of what his company produces. But he said he could not say exactly what chemicals were in the runoff, or floating in the air. "We have about 200 different raw materials that are in our facility," the owner said. "We make about 100 different blends, so it's a constant movement between the seasons and what products are being made." Preliminary testing on the water showed no major health threats. "Two minor compounds were the only things that were detected, and they were very low levels," said a Texas Commission on Environmental Quality member. The owner said investigators believe an electrical spark caused the initial fire. Source: <http://www.nbcdfw.com/news/local/131056128.html>
6. *October 4, Pennsylvania Department of Environmental Protection Northeast Regional Office* – (Pennsylvania) **Pennsylvania DEP fines Northampton cement company more than \$31,000 for emissions violations.** Hercules Cement Co. will pay a \$31,394 fine for sulfur dioxide emissions violations and data availability problems at its facility in Stockertown, Northampton County, Pennsylvania, according to a consent order and agreement announced October 4 by the Pennsylvania Department of Environmental

Protection. The cement manufacturer's kilns exceeded the permitted sulfur dioxide hourly average emissions limit of 500 parts per million for 170 hours during the second, third, and fourth quarters of 2009. The kilns are equipped with monitoring equipment that provide continuous emissions data. Additionally, as part of the facility's air quality permit, 90 percent of each month's monitoring data must be valid. For June 2009, only 81 percent of data were considered valid, due to a system malfunction. Quality assurance, calibration testing, and accuracy calculations are used to determine if a given hour's worth of continuous monitoring data reflects actual emissions. The fine will be paid to the state's clean air fund.

Source: <http://www.sacbee.com/2011/10/04/3959737/pennsylvania-dep-fines-northampton.html>

7. *October 3, Chemical & Engineering News* – (National) **States continue to ban chemicals.** Fueled by consumer concerns about exposure to toxic chemicals, state legislatures in 2011 have continued a trend of recent years by banning specific uses of certain compounds. Thus far this year, lawmakers in six states have adopted laws to restrict bisphenol A (BPA), a phosphate-based flame retardant, according to Safer States, a group that tracks chemical legislation in states. Two states broke new ground on chemical policy this year. New York became the first state to prohibit the use of tris (2-chloroethyl) phosphate in children's goods. And although four other states adopted measures to stop use of BPA in certain products for babies and toddlers, Connecticut became the nation's first state to ban this chemical from thermal paper used in cash register tapes and other receipts. Four other states took action against BPA. Three states, Maine, Delaware, and California, moved to bar BPA in baby bottles and cups for young children. They joined eight other states with similar bans. Maryland, meanwhile, banned sales of infant formula in containers with more than 0.5 part per billion of BPA. Source: <http://pubs.acs.org/cen/government/89/8940gov3.html>

For more stories, see items [2](#), [9](#), [19](#), [26](#), and [27](#)

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

## **Nuclear Reactors, Materials and Waste Sector**

Nothing to report

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

## **Critical Manufacturing Sector**

8. *October 5, WHBL 1330 Sheboygan* – (Wisconsin) **Update: Work as usual in Kohler Foundry.** It was work as usual in the Kohler Company Foundry in Kohler, Wisconsin, October 5 after a fire disrupted the operation the night before. A company spokeswoman said the first shift reported as usual, noting Kohler was still assessing the situation. She said no one was injured and there was no damage estimate. The fire broke out about 11:30 p.m. October 4 after molten metal either spilled or leaked in the foundry. The foundry was evacuated and shut down for a time while the Kohler

Company Fire Brigade, the Kohler Fire Department, and 3 other volunteer departments responded. They encountered smoke and flames, and bystanders reported hearing small explosions. The fire was extinguished and firefighters cleared the scene early October 5.

Source: <http://whbl.com/news/articles/2011/oct/05/fire-shuts-down-the-kohler-foundry/>

9. *October 4, U.S. Department of Labor* – (Alabama) **US Department of Labor’s OSHA cites US Pipe and Foundry Co. for 27 safety violations at Bessemer, Ala., plant; \$85,000 proposed in penalties.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) October 4 cited U.S. Pipe and Foundry Co. for 27 safety violations at its Bessemer, Alabama manufacturing plant. Proposed penalties total \$85,000. Sixteen serious violations with \$76,000 in penalties involve allowing: water on the floor near machinery and without needed drainage; an uneven floor surface that had gaps; an uncovered hole in the floor; four instances in which machinery lacked guards; a control panel for a grinder that was not marked; stairs that were missing an intermediate railing; steps that were damaged; an unsecure scaffold platform; a scaffold plank that was improperly set on a scaffold; a crane that was not marked with its rated load capacity; and drums containing chemicals that were not labeled. Furthermore, an employee was observed operating a forklift without using a seat belt, and forklifts were operated that did not have working flashing lights or alarm signals for backing up.

Source:

[http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=20814](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=20814)

For another story, see item [36](#)

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

## **Defense Industrial Base Sector**

Nothing to report

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

## **Banking and Finance Sector**

10. *October 5, Help Net Security* – (International) **SpyEye Trojan hijacks mobile SMS security for online fraud.** A stealth new attack carried out by the SpyEye Trojan circumvents mobile SMS security measures implemented by many banks, Help Net Security reported October 5. Using captured code, Trusteer found a two-step, Web-based attack that allows fraudsters to change the mobile phone number in a victim’s online banking account and reroute SMS confirmation codes used to verify online transactions. This attack, when successful, enables the thieves to make transactions on the user’s account and confirm them without the user’s knowledge. In the first step of the attack, SpyEye steals online banking log-in details. This allows fraudsters to access the account without raising red flags. In the second step, SpyEye changes the victim’s

phone number of record in the online application to one of several random, attacker-controlled numbers. To complete the operation, the attacker needs the confirmation code sent by the bank to the customer's original phone number. To steal this code, SpyEye injects a fraudulent page in the customer's browser that appears to be from the online banking application. The fake page purports to introduce a new security system "required" by the bank and for which customers must register. The page explains the customer will be assigned a unique telephone number and will receive a special SIM card via mail. Next, the user is told to enter the confirmation number they receive on their mobile telephone into the fake Web page to complete the registration process for the new security system. This allows the criminals to steal the confirmation code they need to authorize changing the customer's mobile number. Now the fraudsters can receive all future SMS transaction verification codes for the hijacked account via their own telephone network. This latest SpyEye configuration shows that out-of-band authentication (OOBA) systems, including SMS-based solutions, are not fool-proof. Using a combination of man-in-the-browser injection technology and social engineering, fraudsters can bypass OOBA, and buy themselves more time since the transactions have been verified.

Source: [http://www.net-security.org/malware\\_news.php?id=1864](http://www.net-security.org/malware_news.php?id=1864)

11. *October 4, Reuters* – (International) **Banks losing ground on card security.** U.S. banks are losing ground in the battle to combat credit and debit card fraud, a new report shows, underscoring the growing threat thieves and hackers pose for the financial system. Globally, security is improving in the payment industry, according to data released the week of October 3 by the Nilson Report, a California trade publication. For every \$100 worth of credit and debit card transactions last year, 4.46 cents were lost to fraud worldwide in 2010, down from 4.71 cents in 2009. But many of the security gains were at banks in Europe and Asia, which have adopted stricter security procedures such as issuing cards with computerized chips to help verify purchases, said the publisher of the Nilson Report. Meanwhile, U.S. banks and merchants have balked at the expense of conversion. As a result, fraud in the United States accounted for 47 percent of global fraud losses last year — up from about 46.5 percent in 2009, and 44 percent in the middle of the last decade, he said. Total fraud losses worldwide were \$7.6 billion in 2010, up 10 percent from 2009, the report found.

Source: <http://www.reuters.com/article/2011/10/04/us-banks-security-idUSTRE7935XO20111004>

12. *October 4, Associated Press* – (New York; International) **NY attorney general files suit claiming currency exchange fraud by Mellon, seeking \$2 billion.** New York's Attorney General (AG) sued Bank of New York Mellon (BNY Mellon) for \$2 billion October 4, claiming it earned that amount over 10 years by defrauding clients in foreign currency exchange transactions. According to the AG's office, BNY Mellon misrepresented rates it would give currency transactions, providing nearly the worst rates of the trading day instead of the best. The case began with a 2009 whistle-blower complaint followed by an investigation. Clients include public pension funds. New York City joined in the lawsuit. On the same day, the U.S. Attorney for the Southern District of New York also announced it had filed a civil fraud lawsuit in Manhattan federal court against the bank, alleging BNY Mellon engaged in a scheme to defraud

custodial clients who used the bank's foreign exchange services from at least 2000 to the present. The suit seeks injunctive relief and hundreds of millions of dollars in civil penalties under the Institutional Reform, Recovery and Enforcement Act of 1989, according to the U.S. attorney's office.

Source: [http://www.washingtonpost.com/business/markets/ny-attorney-general-files-suit-claiming-currency-exchange-fraud-by-mellon-seeking-2-billion/2011/10/04/gIQANxjmLL\\_story.html](http://www.washingtonpost.com/business/markets/ny-attorney-general-files-suit-claiming-currency-exchange-fraud-by-mellon-seeking-2-billion/2011/10/04/gIQANxjmLL_story.html)

13. *October 4, KREM 2 Spokane* – (Northwest) **Bad hair bandit admits to 20 bank robberies.** Court documents, newly filed October 4, said the “Bad Hair Bandit” admitted to almost all of the 21 bank robberies she is accused of committing throughout the Northwest. The bandit was arrested in California in August. She previously worked as a nurse at the Kootenai County Jail, and she and her husband are from Hayden, Idaho. Federal investigators said she robbed 21 banks while wearing different wigs as disguises. They said the string of robberies began in December 2010 at a U.S. Bank in Tacoma, Washington. Investigators said the woman and her husband then hit banks in Spokane and Moses Lake. She was caught in California during a traffic stop after another bank robbery. Authorities said she had \$8,000 in her car, and bystanders took down the make and model of her car as well as partial plate numbers. She has admitted involvement with at least 20 of the robberies. In total, investigators said the couple stole almost \$49,000. She is charged by the criminal complaint filed in Sacramento, California. Her first court appearance in U.S. district court has not yet been set. Source: <http://www.krem.com/news/crime/Bad-hair-bandit-admits-to-20-bank-robberies-131102618.html>
14. *October 4, WCTI 12 New Bern* – (North Carolina) **Two Bank of America bomb threats within 15 minutes.** Two Bank of America branches reported bomb threats within 15 minutes of each other October 3, according to Greenville, North Carolina, police case reports. A police report showed the first bomb threat was reported at 11:10 a.m. from the Bank of America on 1908 S.E. Greenville Boulevard. A second bomb threat was reported at 11:24 a.m. from the Bank of America on 2000 Stantonsburg Road, according to another report. Both bomb threats, which are felonies in North Carolina, turned out to be false, stated the reports. They list the first threat as “inactive”, while the second one is listed as still under investigation. Source: <http://www.wcti12.com/news/29390765/detail.html>

For another story, see item [1](#)

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

## **Transportation Sector**

15. *October 5, WPVI 6 Philadelphia and Associated Press* – (New York; New Jersey) **Pilot in fatal NYC chopper crash was experienced.** The man at the helm of a private helicopter that crashed into the East River between New York and New Jersey, killing one passenger and injuring three others October 4, was an experienced commercial pilot who owns a company that manages a local airport. Investigators were still trying

to determine why the helicopter went down shortly after takeoff from a riverbank heliport. Emergency crews arrived within seconds of the crash to find the helicopter upside-down in the water with just its skids showing on the surface. The pilot and three passengers were bobbing, and witnesses reported a man diving down, possibly in an attempt to rescue the remaining passenger. New York Police Department divers pulled the last passenger, age 40, from the water about 90 minutes after the Bell 206 Jet Ranger went down at around 3:30 p.m. She was pronounced dead at the scene. The crash triggered a massive rescue effort, with a dozen boats and divers going into the water. Police officers doing a counterterrorism drill nearby jumped into the water wearing their uniforms, and without any rescue equipment they pulled the passengers to shore. Fire department rescue paramedics revived two passengers, who were in critical condition; another was stable. All were hospitalized. The pilot swam to shore and was uninjured.

Source: [http://abclocal.go.com/wpvi/story?section=news/national\\_world&id=8379759](http://abclocal.go.com/wpvi/story?section=news/national_world&id=8379759)

16. *October 5, WCAU 10 Philadelphia* – (New Jersey) **Slashed tires put the brakes on NJ buses.** Vandals slashed the tires of all the vehicles at the bus depot on Route 38 in Cherry Hill, New Jersey, overnight October 5, causing the Burlington County Transportation System bus service to shut down for the day. The Burlington County Transportation system confirmed there would be no buses running October 5. Those affected are the BurLink fixed route and paratransit for seniors and the disabled. Authorities said vandals slashed 106 tires on 31 buses. It is estimated the company will lose more than \$31,000 because of the incident. Police are investigating.

Source: <http://www.nbcphiladelphia.com/news/local/Slashed-Tires-Put-the-Breaks-on-NJ-Bus-Service-131128288.html>

17. *October 4, CNN* – (Arizona) **1 dead, 4 critically hurt after Arizona dust storm triggers pileups.** One person was killed and four critically injured October 4 in a series of highway pileups triggered by a dense dust storm on Interstate 10 in central Arizona, a state law enforcement official said. The dust storm moved through the Pichacho Peak area, about 40 miles north of Tucson, at about 12:15 p.m. and caused “minimal visibility” on a stretch of Interstate 10 there, a spokesman for the Arizona Department of Public Safety (DPS) said. He said 16 vehicles were involved in the chain reaction accidents. “We closed the eastbound lanes to allow emergency responders access to the scene,” he said. “Due to the poor visibility, all patients were transported by ground ambulance to Tucson area hospitals.” The dust continues to cause a major hindrance to DPS officers and other rescue personnel, the spokesman added. Another pileup involving eight vehicles, occurred about 90 minutes later, 20 miles to the south on I-10, he said. Two people were critically injured in that incident, which occurred on the eastbound lanes of I-10. The spokesman said he could not estimate when the interstate would reopen in either direction.

Source: <http://www.cnn.com/2011/10/04/us/arizona-dust-storm/>

18. *October 4, Associated Press* – (Texas) **Houston METRO rail hits dump truck, 15 injured.** Authorities said 15 people were injured October 4, when a light rail train derailed after striking a dump truck that ran a red light in downtown Houston. Houston Metro officials said the train operator, 13 passengers, and the truck driver were



transported to hospitals with minor injuries. Metro officials told the Houston Chronicle the truck driver could not see the red light because of the reflection of the sun. Houston police said a hazardous materials unit contained a fuel leak from the dump truck.

Source: <http://www.wtaw.com/2011/10/04/houston-metro-rail-hits-dump-truck-15-injured/>

19. *October 4, Denver Post* – (Colorado) **CSP: Slick material that led to crashes on I-70 is water plant waste.** A truck hauling waste from a water treatment plant leaked October 3, leaving a slippery trail and traffic accidents on the highway, investigators said. The truck that left the slick material on a portion of eastbound I-70 in Wheat Ridge, Colorado, and a nearby section of I-76, is an EDS Waste Solutions vehicle, the Wheat Ridge Police Department said. The driver was given a traffic ticket for a spilled load on the highway. About a dozen vehicles, including at least three motorcycles, were involved in the highway crashes, which knotted rush hour traffic on the highway near Carr Street. The eastbound lanes were closed for almost 3 hours. The slick substance also caused a single motorcycle accident on I-76 in Adams County, the state patrol said. A Colorado State Patrol spokesman said all of the injured people taken to the hospital October 3 have been released.

Source: [http://www.denverpost.com/breakingnews/ci\\_19037552](http://www.denverpost.com/breakingnews/ci_19037552)

20. *October 4, KMBC 9 Kansas City* – (Missouri) **Multiple train cars derail in Carroll County.** A train derailment October 4 blocked Highway 10 in Carroll County, Missouri, local fire department officials said. A Norfolk Southern spokesman said 10 cars went off the track at about 3:30 p.m. The cars were carrying auto parts. Highway 10 opened late the afternoon of October 4.

Source: <http://www.kmbc.com/news/29387826/detail.html>

For another story, see item [2](#)

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

## **Postal and Shipping Sector**

Nothing to report

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

## **Agriculture and Food Sector**

21. *October 5, Food Safety News* – (International) **Europe cancels consumer caution about sprouts.** The European Food Safety Authority (EFSA) October 4 dropped its consumer advisory against eating raw sprouts and growing sprouts from seed at home, and recommended consumers refer to the various national food safety agencies for specific guidance on sprouts. EFSA said the reason for canceling the advisory was fenugreek seeds from Egypt, the most likely cause of the massive outbreak of E. coli 0104:H4 centered in Germany in the spring of 2011, are no longer on the market. The agency also said its biological hazards panel, by request from the European

Commission, was carrying out a risk assessment on the EU production chain for sprouts and sprouting seeds, and would publish a scientific opinion “in the coming weeks.” In a wrap-up report on the E. coli O104:H4 outbreak, which ended July 26, EFSA said there were at least 3,134 cases and 47 deaths. E. coli O104:H4 was never detected in any of the batches of suspect fenugreek seeds, something that “is not unexpected,” according to EFSA, because it was possible the contaminated seeds were no longer in stock when sampling took place, or that the pathogen was present at such a low level that isolating the organism was not possible.

Source: <http://www.foodsafetynews.com/2011/10/europe-cancels-consumer-caution-about-sprouts/>

22. *October 5, CNN* – (National) **Death toll now 18 from tainted cantaloupes.** The number of deaths linked to cantaloupe contaminated with the *Listeria monocytogenes* bacteria has risen to 18, the U.S. Centers for Disease Control and Prevention (CDC) said October 4. At least 100 cases of listeria have been reported in 20 states, the agency said. Health officials have said the number of cases could continue to grow, citing reporting lags and the fact the disease can develop slowly in some people, taking up to 2 months. The listeria outbreak is the deadliest food-borne illness outbreak in the United States since 1998. Five people each have died in New Mexico and Colorado from consuming the tainted fruit, along with two people each in Kansas and Texas, and one each in Maryland, Missouri, Nebraska, and Oklahoma, the CDC said. Cases have also been reported in Alabama, Arkansas, California, Idaho, Illinois, Indiana, Montana, North Dakota, Texas, Virginia, West Virginia, Wisconsin, and Wyoming. The grower, Jensen Farms of Granada, Colorado, issued a voluntary recall of its Rocky Ford brand cantaloupes September 14.

Source: [http://www.cnn.com/2011/10/04/health/cantaloupe-deaths/index.html?hpt=hp\\_t2](http://www.cnn.com/2011/10/04/health/cantaloupe-deaths/index.html?hpt=hp_t2)

23. *October 5, Food Safety News* – (International) **Soybean meal, flour recalled for Salmonella.** A Michigan company is recalling 2,623 40-pound bags, 360 1,500-pound totes of soybean flour, and 924 .08-ton loads of bulk soy meal because they may be contaminated with *Salmonella*, Food Safety News reported October 5. The soy meal and flour was used to manufacture human and animal food, and had been distributed since November 2010. Thumb Oilseed Producer’s Cooperative of Ubly, Michigan said in a news release the recall resulted from routine sampling conducted by the company and U.S. Food and Drug Administration (FDA) that revealed *Salmonella* in finished product, and the manufacturing plant. Thumb Oilseed is cooperating with the FDA. The soy flour was distributed in 40-pound paper bags under the names: Nex Soy (lot numbers TF112310 thru TF033011) and Soy Beginnings (product code 285100-NFB; lot numbers TF112310 thru TF033011). The soy flour was also distributed in 1,500-pound polyurethane totes under the name: Soy Beginnings (product code 285100-NFT, lot numbers TF112310 thru TF082311). The soy meal was distributed as .08 ton loads after custom processing with lot numbers O011711 thru O081711. The recalled soybean flour and meal was distributed from November 2010 to September 2011 to a limited group of wholesale customers in Illinois, Vermont, Minnesota, Pennsylvania, Wisconsin, New Hampshire, and Canada.

Source: <http://www.foodsafetynews.com/2011/10/soybean-meal-flour-recalled-for-salmonella/>

24. *October 4, Associated Press* – (Oregon) **Irrigation ditch breach endangers Ore. salmon eggs.** Biologists were hoping wild spring chinook in the Rogue River near Grants Pass, Oregon, “dodged a bullet” after a break in an irrigation ditch sent suffocating muddy water coursing over millions of freshly laid eggs that represent a big chunk of future runs, the Associated Press reported October 4. If fine particles of clay settled around the millions of eggs laid in gravel beds in recent weeks, the eggs could suffocate and die, an Oregon Department of Fish and Wildlife fish biologist said October 4. Only about half of the estimated 4,700 adult females in this year’s wild spring run have laid their eggs so far. The rest should be able to dig clean nests in the river gravel even if silt settled over the spawning beds. Officials said they also hope the clay particles were fine enough to stay suspended in the water far enough downstream so eggs would not be suffocated.

Source: <http://www.oregonlive.com/newsflash/index.ssf/story/irrigation-ditch-breach-endangers-ore-salmon-eggs/4e939e08a50f4a22a8bd2263002d894b>

For another story, see item [27](#)

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

## **Water Sector**

25. *October 5, Salem News* – (Massachusetts) **Boil water order in Wenham.** Residents in Wenham, Massachusetts, were advised to boil their water after E. coli bacteria was detected in the public water supply October 4, the Salem News reported. Wenham water tested positive for coliform bacteria at all sites in the water distribution system during a routine test the week of October 3; two samples also tested positive for E. coli. Wenham draws its water supply from groundwater fed by the Ipswich and Miles rivers, said the town administrator. The cause of the bacteria in the water supply is under investigation. The heavy rain and flooding October 3 could have been a factor, officials said. Once two successive water tests come back clean, the boil water order will be lifted, the earliest that could be is October 7, the town administrator said. Wenham firefighters began running fire hydrants around town to flush the system October 4, and water department personnel were chlorinating the entire water system and flushing lines.

Source: <http://www.salemnews.com/local/x555350176/Boil-water-order-in-Wenham>

26. *October 4, WTOL 11 Toledo* – (Michigan) **Detroit sewage contributing to Lake Erie algae bloom.** Environmentalists raised a red flag after Detroit, Michigan released billions upon billions of gallons of raw and diluted sewage into Lake Erie in 2011, WTOL 11 Toledo reported October 4. The city is home to the single largest wastewater plant in the country. According to the Lake Erie Waterkeeper, Detroit unloaded nearly 30 billion gallons of raw and partially treated sewage into the Detroit River during the first 7 months of 2011. The Detroit River flows into Lake Erie. The waterkeeper followed Detroit’s discharges on the Michigan Department of Environmental Quality’s

Web site and saw the numbers add up. The Detroit Water and Sewerage Department said the majority of the water released is treated, and the city is in compliance with Michigan Environmental Quality rules. The increased number of sewer overflows in 2011, when compared to 2010, occurred because of heavy rain.

Source: <http://www.wtol.com/story/15617327/detroit-sewage-contributing-to-lake-erie-algae-bloom>

27. *October 4, WCNC 36 Charlotte* – (North Carolina) **Sewage leak contaminates Briar Creek.** Residents in Charlotte, North Carolina, were told to stay away from Briar Creek for a few days after a wastewater leak caused contamination, WCNC 36 Charlotte reported October 4. Charlotte-Mecklenburg Utilities (CMU) said a wastewater pipe broke October 2 after recent rain that caused erosion to the creek bank, spilling more than 180,000 gallons of sewage into the creek. The spill has killed 3,000 fish and is endangering more. CMU was trying to fill the creek with clean water to give the remaining fish a good chance at survival. Officials said the goal was to get the pipe fixed and stabilize the creek bank, which should take about 10 days.

Source: <http://www.wcnc.com/news/neighborhood-news/Sewage-leak-contaminates-Briar-Creek-131117713.html>

For more stories, see items [5](#) and [36](#)

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

## **Public Health and Healthcare Sector**

28. *October 4, Federal Computer Week* – (National) **VA errors compromise identity verification credentials.** The U.S. Veterans Affairs department (VA) may have issued more than 157,000 personal identification credentials without authenticating the identity of the individuals who received them, according to a new report from the Office of Inspector General. Overall, the VA may have issued at least 147,000 credentials without determining whether applicants are known or suspected terrorists, and presented genuine and unaltered identity source documents, the assistant inspector general wrote in a September 30 report. Also, VA may have issued at least 5,100 credentials without verifying applicants' background investigations, and 5,600 credentials where staff circumvented separation of duty control requirements. The assistant inspector general for audits and evaluations recommended the department immediately direct the VA Enrollment Centers to stop issuing new credentials until the control deficiencies are addressed. VA officials said they had taken immediate action to mitigate the risks uncovered in the report by reviewing the questionable credentials. The assistant inspector general estimated the cost to correct the deficiencies at approximately \$6.7 million, and said costs would continue to increase if additional credentials were issued.

Source: <http://fcw.com/articles/2011/10/04/va-issued-157000-questionable-id-credentials-oig-says.aspx>

29. *September 23, MedPage Today* – (National) **Medical identity theft a growing problem.** According to a recent report on a nationwide survey of 600 executives from

U.S. hospitals, doctors' organizations, health insurance companies, pharmaceutical manufacturers, and life sciences companies, accounting firm PricewaterhouseCoopers (PwC) found medical identify theft is the fastest-growing form of identity theft, affecting 1.42 million Americans in 2010, and costing more than \$28 billion. Theft accounted for 66 percent of the publicly reported security breaches documented since 2009, which included stolen laptops, stolen smart phones, using patient data to submit fraudulent claims, and people seeking medical care in another person's name. The single most commonly reported breach in the security of patients' private health information was improper use of patient data by a person who works for a doctor's office, hospital, insurance company, or life sciences organization. The breaches ranged from an employee leaving private documents out in plain sight, to making improper comments on Facebook, or even talking in the elevator about a person's protected health information. Nearly four out of 10 doctors and hospitals surveyed have caught a patient trying to use someone else's identity to obtain healthcare services. Patients seeking medical services under someone else's name was the second most common privacy or security issue reported by healthcare providers. Rounding out the top three most common breaches was improper transfer of files containing personal health data to people who were not authorized to view the information. One in four insurers reported improperly transferring files that contained protected health information. Source:

<http://www.medpagetoday.com/PracticeManagement/InformationTechnology/28696>

For another story, see item [31](#)

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

## **Government Facilities Sector**

30. *October 5, WMUR 9 Manchester* – (New Hampshire) **Exeter High evacuated for acid leak.** Exeter High School in Exeter, New Hampshire was evacuated October 4 after a janitor crushed waste in a trash bin that had two cans of sulfuric acid in it, according to school officials. Some of the acid leaked out, and officials were concerned about vapors causing injuries. The students were put on lockdown at first before they were sent home early for the day. About 300 staff members were also evacuated. Three people, including the janitor, were treated for exposure to the acid at a local hospital, and two others were treated at the school. The school said no students were exposed. School officials said the acid is commonly used for lab experiments, but for some reason, the cans were not emptied, and the acid was not neutralized. Classes were expected to resume October 5.

Source: <http://www.wmur.com/r/29384531/detail.html>

For more stories, see items [31](#), [33](#), [35](#), and [44](#)

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

## Emergency Services Sector

31. *October 5, Press of Atlantic City* – (New Jersey) **Atlantic City casinos give police access to surveillance systems; will share video, voice, text via Internet.** Police will soon have access to Atlantic City, New Jersey casinos’ surveillance systems to help them fight crime in the Tourism District, the Press of Atlantic City reported October 5. By early next spring, all gaming halls will be part of Mutualink, a radio and wireless interoperability system that will allow law enforcement access to the closed-circuit televisions in each casino, as well as hospitals and other public institutions. State officials said access to the cameras will help emergency responders in the event of a terrorist attack or other public safety event. The agreement between casinos and the state Division of Gaming Enforcement (DGE) , announced October 4, follows the highly publicized carjacking last month at the Trump Taj Mahal Casino Resort that left a Middlesex County man dead, and his female companion wounded. The DGE has been working with state police and the office of homeland security and preparedness to activate the emergency system in each casino that will allow dispatchers, police, fire, emergency medical services, and other public safety agencies to share voice, video, text, and files across a secure Internet connection.  
Source: [http://www.pressofatlanticcity.com/news/press/atlantic\\_city/atlantic-city-casinos-give-police-access-to-surveillance-systems-will/article\\_a6c83b30-eee5-11e0-9637-001cc4c002e0.html](http://www.pressofatlanticcity.com/news/press/atlantic_city/atlantic-city-casinos-give-police-access-to-surveillance-systems-will/article_a6c83b30-eee5-11e0-9637-001cc4c002e0.html)
32. *October 5, Associated Press* – (Connecticut; National) **Responders train for hybrid, electric car rescues.** In 2010, the National Fire Protection Association received a \$4.4 million grant from the U.S. Department of Energy to develop a training program to instruct fire department personnel on the potential hazards they may encounter at a motor vehicle accident with all-electric and hybrid vehicles, or cars with both combustion engines and battery packs. Instructors from 38 fire departments across Connecticut recently attended a train-the-trainer course at the Connecticut Fire Academy to view procedures in handling all-electric and hybrid vehicle accidents, the Associated Press reported October 5. The fire association took the data and created a 2-page Emergency Response Guide, so emergency crews could focus on critical information when they arrive at the scene of an accident. The fire association instructor said the high strength steel being used in electric and hybrid cars is creating additional concerns. Although the cars are 75 percent lighter, they are now 15 percent stronger, making it difficult for firefighters to cut through to reach anyone trapped inside, he said. Another possible danger is a battery breach, he said, in which fluids can leak onto the ground, creating an environmental hazard.  
Source: <http://www.courant.com/community/manchester/hc-ap-ct-electriccarrescueoct05,0,3939571.story>
33. *October 4, DCist.com* – (District of Columbia) **D.C. officials get priority phone access during emergencies.** To allow city officials to better respond to emergencies and disasters, October 4 members of the Washington D.C. Council were given special cards that allow their calls to take priority during moments of heavy call volume. The cards, which are part of the DHS’s Government Emergency Telecommunications Service (GETS), provide “emergency access and priority processing in the local and

long distance segments of the Public Switched Telephone Network (PSTN).” GETS is “intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased,” according to DHS. The agency said the GETS card is designed to provide 90 percent call completion rates when call volume is eight times higher than usual.

Source: [http://dcist.com/2011/10/dc\\_officials\\_get\\_priority\\_phone\\_acc.php](http://dcist.com/2011/10/dc_officials_get_priority_phone_acc.php)

34. *October 4, Durango Herald* – (Colorado) **Lightning disables 911 tower.** Lightning believed to have struck October 2 or early October 3 disabled a radio tower with multiple antennas on Grassy Mountain between the Forest Lakes subdivision and Vallecito Reservoir near Bayfield, Colorado. A statewide communications system that operates on 800 megahertz, and the local VHF emergency dispatch system that serves the Upper Pine Fire Protection District (UPFPD) were affected, UPFPD’s chief said October 4. The La Plata County Sheriff’s Office communications van, stationed at Vallecito, has taken up the slack, providing a link for local emergency service, the chief said. “As a result, there has been no interruption, no lapse, in local emergency response,” he said, noting 911 calls will be answered by central dispatch in Bodo Industrial Park. The chief said parts to repair the radio tower, which operates on solar panels with an engine-powered backup, are being delivered from Grand Junction. The 800-megahertz system could be out for up to 10 days.

Source: <http://durangoherald.com/article/20111005/NEWS01/710059913/-1/s>

35. *October 4, St. Petersburg Times; Associated Press* – (National) **Tampa takes heed as cyber threat accompanies Occupy Wall Street protest.** The Occupy Wall Street protest is coming to Tampa, Florida, and it appears a notorious hacker group has threatened Tampa police online assets, the St. Petersburg Times and Associated Press reported October 4. In a YouTube video, a masked man warns police brutality will be the department’s downfall. “If you wish to have the Tampa Police Department alive as a whole — and this is metaphorically speaking — then stay away from the protesters,” he said. The video is attributed to “hactivist” group Anonymous, best known for its cyber attacks on Sony, Bank of America, and the Iranian government. It is unclear if Anonymous is truly behind the video, or if the masked man is acting alone. Nonetheless, the city is preparing. It has to, Tampa’s chief information officer said, given Anonymous’ previous cyber hacking successes. The city already has intrusion detectors and firewalls in its systems that officials constantly update. They do not plan to buy new products, he said. Instead, employees will monitor the systems more closely this week.

Source: <http://www.tampabay.com/news/publicsafety/city-takes-heed-as-cyber-threat-accompanies-occupy-wall-street-protest-set/1195089>

36. *October 3, Baltimore Brew* – (Maryland) **Fire department confirms hydrants didn’t work at Sparrows Point.** The Baltimore County Fire Department confirmed October 3 that fire crews responding to a fire at the Sparrows Point steel mill in Maryland were faced with non-working fire hydrants. Firefighters used water on several responding engines and dispatched a high-capacity tanker from the Kingsville Volunteer Fire Company September 30, the chief public safety officer said. While the absence of

working hydrants “probably had minimal impact on the eventual damage to the building,” the officer said it “subjected our personnel to additional risk.” It also meant the department had to commit more personnel and equipment to fighting the fire. It took nearly 2 hours to get the fire under control. Once the fire began — reportedly from sparks mixing with oil in the basement of the mill — “it quickly escalated beyond the plant’s ability to handle it, and the fire department was called,” according to officials. Source: <http://www.baltimorebrew.com/2011/10/03/fire-department-confirms-hydrants-didnt-work-at-sparrows-point/>

For more stories, see items [4](#), [15](#), and [45](#)

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

## **Information Technology Sector**

37. *October 5, H Security* – (International) **Chrome 14 update brings Flash 11, closes security holes.** Google has released version 14.0.835.202 of Chrome, a maintenance and security update for all supported platforms. This stable channel update includes the new Flash Player 11 release and addresses a total of 9 vulnerabilities. Rated as “critical” by Google, a memory corruption problem has been fixed in the shader translator. Other holes closed include eight “high-risk” bugs ranging from a use-after-free error in text line box handling and stale fonts in text handling, to a cross-origin problem, lifetime and threading issues in audio-node handling, and use-after-free and memory corruption exploits in V8, the browser’s JavaScript engine. However, Google’s fix for the SSL/TLS vulnerability has yet to make it from the development version to the stable branch.  
Source: <http://www.h-online.com/security/news/item/Chrome-14-update-brings-Flash-11-closes-security-holes-1354670.html>
38. *October 5, H Security* – (International) **Firefox and SeaMonkey users warned to disable McAfee ScriptScan.** A major incompatibility between Mozilla’s browsers Firefox and SeaMonkey, and McAfee’s ScriptScan plug-in has caused “a high volume of crashes,” according to Mozilla. The problem first came to light in September, when members of the McAfee forum began reporting problems with version 14.4.0 of ScriptScan, a tool that checks Web pages, as they are loaded into the browser, for malicious code. This is the first time since July that Mozilla has found it necessary to block a plug-in. All versions of Firefox and SeaMonkey are affected by the problem, as are all current versions of McAfee ScriptScan. Mozilla recommends ScriptScan users disable the browser plug-in. The issue only affects version 7 of the browsers, according to a McAfee spokesperson.  
Source: <http://www.h-online.com/security/news/item/Firefox-and-SeaMonkey-users-warned-to-disable-McAfee-ScriptScan-1355098.html>
39. *October 4, H Security* – (International) **Cisco patch day closes critical vulnerabilities.** Cisco has published 10 security advisories as part of its bi-annual patch day. The advisories resolve a number of security vulnerabilities. The most serious vulnerability (CVSS 10) addressed was in Catalyst switches running the company’s



iOS network operating system software. A bug in the Smart Install remote maintenance feature allowed remote attackers to execute arbitrary code on affected switches. The other advisories fix denial-of-service vulnerabilities in iOS, Unified Communications Manager, and 1000 series routers. Cisco has released updates that fix these vulnerabilities; workarounds exist for some of the problems. Cisco has also fixed the backdoor vulnerability in its Identity Services Engine identity-management software. Source: <http://www.h-online.com/security/news/item/Cisco-patch-day-closes-critical-vulnerabilities-1354156.html>

40. *October 4, IDG News Service* – (International) **XSS Web attacks could live forever, researcher warns.** Web sites that accidentally distribute rogue code could find it harder to undo the damage if attackers exploit widespread browser support for HTML5 local storage, and an increasing tendency for heavy users of Web apps never to close their browsers. If browsers do not provide a mechanism for Web sites to recover from certain cross-site scripting attacks, the attacks could become invincible and the site at the origin of the attack remain compromised indefinitely, a vulnerability researcher and Google security engineer warned October 1. The scope of client-side programming languages such as JavaScript within browsers is limited by a critical security concept known as the same-origin policy. This prevents scripts running on certain Web pages from interfering with Web sites opened in separate tabs or windows. In the case of cross-site scripting (XSS), attackers manage to insert rogue JavaScript code in targeted pages, where it is then executed in the context of their origin, defined by the domain, the protocol, and the port number. JavaScript is very powerful and is used in most Web-based attacks. Despite this, browsers do not currently provide a mechanism to invalidate such code, something that would provide compromised Web sites with a way to request a clean slate once they had resolved the problem. A normal response to XSS attacks is to patch the vulnerability, invalidate session cookies so that everyone is forced to re-authenticate, and optionally force a password change. But this is not enough, because, according to the researcher, once compromised a Web origin can stay tainted indefinitely.

Source:

[http://www.computerworld.com/s/article/9220511/XSS\\_web\\_attacks\\_could\\_live\\_forever\\_researcher\\_warns](http://www.computerworld.com/s/article/9220511/XSS_web_attacks_could_live_forever_researcher_warns)

41. *October 4, The Register* – (International) **Facebook to scrub itself clean of filthy malware links.** Facebook has recruited Websense to scan its social network for links to malicious sites. Scammers are increasingly using Facebook as a means to drive traffic towards malware and exploit portals or Internet scam sites. In response, Facebook is tapping Websense for technology that will analyze the jump off points to links. Cloudy technology will assign a security classification to sites, presenting users with a warning if the location is considered dangerous. This warning page will explain why a site might be considered malicious. Users can still proceed, at their own risk, to potentially dodgy sites. Before, individual users had the option to add additional security filtering apps, such as Bitdefender Safego, to their profiles as a means to scan for spam and malicious links. Facebook is now offering this type of technology by default as an extension of its previous relationship with Websense.

Source: [http://www.theregister.co.uk/2011/10/04/facebook\\_websense\\_scam\\_scanning/](http://www.theregister.co.uk/2011/10/04/facebook_websense_scam_scanning/)

42. *October 4, The Register* – (International) **Check your machines for malware, Linux developers told.** Following a series of intrusions that hit the servers used to maintain and distribute the Linux operating system, project elders have advised all developers to check their Linux machines for signs of compromise. E-mails sent September 30 by Linux kernel's lead developers arrived as volunteers with the open-source project worked to bring LinuxFoundation.org, Linux.com, and Kernel.org back online following attacks that gained root access to the multiple servers that host the sites. Among other things, project leaders are requiring all developers to regenerate the cryptographic keys used to upload source code to the site, and to ensure their systems are free of rootkits and other types of malware.  
Source: [http://www.theregister.co.uk/2011/10/04/linux\\_repository\\_res/](http://www.theregister.co.uk/2011/10/04/linux_repository_res/)

For more stories, see items [10](#), [35](#), and [44](#)

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [sos@us-cert.gov](mailto: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

See items [10](#), [31](#), [34](#), and [41](#)

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

## Commercial Facilities Sector

43. *October 5, Associated Press* – (Iowa) **Downtown Iowa City fire caused millions in damage.** A fire that damaged a downtown Iowa City, Iowa bagel shop and other buildings caused millions of dollars in damage, the Associated Press reported October 5. That is the assessment from the Iowa City fire marshal, who inspected the damaged buildings October 4. He said the cause of the fire would not be determined the week of October 3. The fire marshal and others began sifting through debris October 4 as they began to look for the cause of the fire that damaged the Bruegger's Bagels shop in September. The fire and smoke also damaged a handful of nearby businesses and apartments.  
Source: <http://www.chicagotribune.com/news/chi-ap-ia-iowacityrestaurant,0,172778.story>
44. *October 5, msnbc.com; Associated Press* – (California) **Manhunt after 2 die in Calif. workplace shooting.** Authorities were searching door to door with guns drawn in a neighborhood about 5 miles from the Cupertino, California quarry where a gunman killed two and wounded six at a morning meeting October 5. Schools were on

lockdown or closed in Cupertino as SWAT teams sought the 47-year-old suspect. He also is suspected of wounding a woman in an attempted carjacking in Cupertino more than 2 hours later. A Santa Clara County sheriff's lieutenant said the suspect was at the routine safety meeting at 4:30 a.m., became disgruntled and left. He said he then returned with a 9 mm handgun and a rifle and started shooting people. In the early afternoon October 5, authorities were searching the quarry for possible victims. About 15 workers were evacuated and being kept at a safe location. The suspect is a San Jose resident who was a truck operator at the Permanente Cement Plant, and also produced and hosted a public access television show for CreaTV in San Jose. After leaving the quarry, the suspect attempted a carjacking at a nearby Hewlett-Packard parking lot, shooting a female driver in the leg. He did not get the car from her. Three of the victims were taken to Santa Clara Valley Medical Center, including the woman shot in the carjacking, a hospital spokeswoman said. One victim was treated and released, while the other two were in fair condition, she said. In nearby Sunnyvale, another injured person was found in a parking lot, reported KNTV 11 San Jose, but it was not clear if that was connected to the workplace shooting. The suspect is described as African American, 5'11", and 260 pounds, with numerous tattoos, according to KNTV. Permanente Cement Plant, owned by Lehigh Hanson, Inc., is a limestone and aggregate mining operation and cement plant.

Source: [http://www.msnbc.msn.com/id/44785704/ns/us\\_news-crime\\_and\\_courts/#.ToyWjnLm9\\_6](http://www.msnbc.msn.com/id/44785704/ns/us_news-crime_and_courts/#.ToyWjnLm9_6)

45. *October 4, Burlington County Times* – (New Jersey) **Hurricane damage forces cancellation of Batsto fair.** Hurricane Irene damage has forced the cancellation of the Country Living Fair in Batsto Village, New Jersey, the Burlington County Times reported October 4. The decision to nix the signature annual event in the historic village in the Wharton State Forest was a safety measure decided upon by officials from the Batsto Citizens Committee, Wharton State Forest, Atlantic County Engineer's Department, New Jersey State Police, and New Jersey State Park Police, according to a letter sent to fair participants. "Response time for an emergency either at Batsto or along the detour could be too long in some cases," according to the letter, which was signed by two committee members. The hurricane affected the main thoroughfares to and from the event, which usually draws an estimated 50,000 people to the village.

Source:

[http://www.phillyburbs.com/news/local/burlington\\_county\\_times\\_news/hurricane-damage-forces-cancellation-of-batsto-fair/article\\_9ec480f4-5e6b-5892-8279-300923ecb3e1.html](http://www.phillyburbs.com/news/local/burlington_county_times_news/hurricane-damage-forces-cancellation-of-batsto-fair/article_9ec480f4-5e6b-5892-8279-300923ecb3e1.html)

46. *October 4, KSTU 13 Salt Lake City* – (Utah) **Concert brawl downtown injures 4, one critically.** It was packed late October 3 at the concert club "In the Venue" in Salt Lake City, Utah when a fight broke out minutes into the show. Four people were injured, one critically, during a fight between concertgoers and several of the band members on stage. A witness said it all started with a group of people who kept antagonizing the band. The altercation, seen on video captured and uploaded to YouTube, shows the lead singer retaliate after apparently being taunted. A witness said after that, some of the audience members who were allegedly tormenting the band, came on stage to fight and the melee broke out on stage, with concertgoers attacking band members. The band

members were not injured and when everything calmed down, they finished the rest of their show. Police have not made any arrests yet, but said the incident is most likely gang related.

Source: <http://www.fox13now.com/news/local/kstu-concert-brawl-downtown-injures-4-one-critically-20111004,0,6694756.story>

For more stories, see items [4](#), [31](#), and [47](#)

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

## **National Monuments and Icons Sector**

47. *October 5, Associated Press* – (Texas) **More than 50 Central TX homes been evacuated as firefighters battle new wildfire.** Firefighters continued battling a wildfire overnight October 4 into October 5 in the same Central Texas county where a destructive fire in September destroyed more than 1,500 homes. Officials were hopeful weather conditions October 5 would let them continue containing the Bastrop County fire that forced 50 homes to be evacuated as a precaution. The fire was about 25 percent contained late in the evening October 4. A Texas Forest Service spokesman said the fire in a heavily forested area near Austin had burned about 1,000 acres. He said six aircraft that have dropped fire retardant on the fire have helped bring it under control. Source: <http://abclocal.go.com/ktrk/story?section=news/local&id=8379555>
48. *October 4, Associated Press* – (Nevada) **Tuscarora evacuation lifted in NV fires.** A wet storm moving into the Sierras promised some help for firefighters battling a series of wildfires across northern Nevada October 4 as crews lifted an evacuation at a small mining town and continued to keep the flames from damaging any homes. A trio of wildfires in north-central and northeast Nevada continued to grow, burning up tens of thousands of acres of prime mule deer and game bird habitat in largely unpopulated parts of the state. But shifting winds October 4 allowed several dozen residents to return to the tiny mining town of Tuscarora after one fire forced mandatory evacuations the night before. A spokeswoman for the multi-agency fire incident team, said the Indian Creek fire “caused a little bit of concern” late October 3. More than 500 firefighters have battled the flames across an area equal to 250 square miles since lightening touched off the fires making up the Dunphy complex September 30 and October 1. In western Nevada, firefighters continued to hold the line on the 1,062-acre Burbank fire in Smith Valley southeast of Gardnerville. It was estimated to be more than one-quarter contained October 4 with full containment projected by October 8. Source: <http://www.sacbee.com/2011/10/04/3960283/tuscarora-evacuation-lifted-in.html>
49. *October 4, Associated Press* – (California) **2,000-acre San Diego wildfire 75 percent contained.** Fire bosses said cooler, wet weather helped firefighters battle a 2,000-acre wildfire in rural San Diego County, California, the Associated Press reported October 4. The latest California Department of Forestry and Fire Protection report early October 4 said the fire 5 miles east of Julian was 75 percent surrounded, or contained. Full containment was expected sometime October 6. The fire battalion chief said there was

no open flame, and firefighters were slowly being demobilized. The firefighting force has been reduced from 1,500 to 1,000. He said cooler weather allowed faster progress on snuffing out hot spots. He said firefighters would be helped by a rainstorm expected October 5. The fire has been burning since October 1 near Shelter Valley, an area south of State Route 78. The cause has not been determined.

Source: <http://www.fresnobee.com/2011/10/04/2563640/2000-acre-san-diego-wildfire-65.html>

50. *October 4, msnbc.com* – (District of Columbia) **Washington National Cathedral to reopen in November.** The Washington National Cathedral will reopen November 12 — more than 2 months after sustaining damage from an August 23 earthquake, according to a statement released October 4. The 30-story central tower had suffered “significant” damage during the earthquake, with three of the fleurs-de-lis shaped corner spires breaking off and falling to the ground. Since its closure, workers have begun placing steel beams in the central tower to stabilize a 550-ton-capacity construction crane. Once workers are able to access the damaged pinnacles, they will be removed. The cathedral confirmed in its statement restoration work would take years and cost tens of millions of dollars, and noted it is trying to raise at least \$25 million to pay for construction and operating costs through 2012.

Source: [http://overheadbin.msnbc.msn.com/\\_news/2011/10/04/8151195-washington-national-cathedral-to-reopen-in-november](http://overheadbin.msnbc.msn.com/_news/2011/10/04/8151195-washington-national-cathedral-to-reopen-in-november)

For another story, see item [45](#)

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

## **Dams Sector**

51. *October 4, Marshall Democrat-News* – (Missouri) **River continues to erode levee in Grand Pass bottoms.** Members of the Saline-Lafayette Levee district of Saline County, Missouri, discovered October 4 another large piece of a private levee located in the Grand Pass bottoms, sloughed off into the Missouri River. A piece of the levee fell into the river August 1 but was saved by dumping large pieces of concrete into the hole. Since then, about 8,000 tons of rock have been used to reinforce the levee. The state emergency management agency said 2,000 more tons of rock were used the week of September 26. By October 4, large pieces of the levee continued to break off into the river. Seven trucks put about 600 tons of rock into the hole after officials made the decision to pull the top off the levee and move it back.

Source: <http://www.marshallnews.com/story/1770230.html>

52. *October 3, KSL 5 Salt Lake City* – (Utah) **Multi-million dollar renovation under way at Echo Dam.** The Echo Dam near Coalville, Utah, is only the latest of a dozen dams in Utah and Wyoming that have been upgraded in recent years as a result of what has been learned about earthquakes, KSL 5 Salt Lake City reported October 3. The goal is to avoid the nightmare situation a moderate earthquake could create: a wall of water racing down Weber Canyon, taking out town after town on its way to Ogden and the Great Salt Lake. The dam was built 80 years ago, when scientists knew a lot less about

earthquakes. If the earthen dam shakes, rock, dirt, and sand under it could liquify, causing it to slump and possibly fail catastrophically. A surprisingly small quake could trigger that catastrophe; above magnitude 5.6, the risk is there. The fix will raise the safe level to magnitude 7.2. Crews plan to excavate to bedrock at the foot of the dam, and widen the dam with compacted dirt and rock. The reservoir will also be lowered and the dam on the upstream side raised. The project is scheduled for completion in 2015 at a cost of at least \$40 million.

Source: <http://www.ksl.com/?nid=148&sid=17513202>

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

## **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](mailto:cikr.productfeedback@hq.dhs.gov) or contact the DHS Daily Report Team at (703)387-2267

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](mailto: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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://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.