



# Homeland Security

## Daily Open Source Infrastructure Report for 1 November 2010

### Current Nationwide Threat Level

ELEVATED



Significant Risk of Terrorist Attacks

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

### Top Stories

- CNN reported suspicious packages found in two locations in the Middle East on planes bound for places of Jewish worship in Chicago, Illinois, October 29, contained explosive material put there by al Qaeda in the Arabian Peninsula, U.S. officials said. (See item [21](#))
- The FBI said October 29 the National Museum of the Marine Corps building in Triangle, Virginia was fired upon for the second time in days, according to CNN. Authorities said previous shots fired at the museum, the Pentagon, and a Marine Corps recruiting station all came from the same weapon. (See item [39](#))

### 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 29, Reuters* – (New Jersey; National) **Conoco Bayway restart delayed about 1 month.** The crude distillation unit at ConocoPhillips' 238,000 barrel-per-day Bayway refinery in New Jersey is not expected to return from planned work until late November 2010, a source familiar with refinery operations said October 29. The unit went down for about 45 days of planned work September 23, with restart expected in early

November. On October 25, a fire at a transformer cut power to the plant, further delaying the restart, which was already 1 week behind schedule and over budget, the source said. Power was restored October 26. The 145,000 barrel-per-day, gasoline-making, fluid-catalytic cracking unit is still under assessment for damage that could have occurred during the cold shutdown. The furnaces were running but there has been no activity on restarting the unit over the past 24 hours, the source said. On October 29, ConocoPhillips was looking to “slowly” bring the hydrofiner back on line.

Source: <http://www.reuters.com/article/idUSN2928195520101029>

2. *October 29, msnbc.com* – (Louisiana) **Halliburton admits skipping test on Gulf well cement.** Halliburton Co. acknowledged October 28 it skipped doing a critical test on the final formulation of cement used to seal the BP oil well that blew out in the Gulf of Mexico. The company, which was BP’s cementing contractor, said BP at the last-minute increased the amount of a critical ingredient in the cement mix. While an earlier test showed the cement was stable, the company never performed a stability test on the new blend. The cement’s failure to prevent oil and gas from entering the well has been identified as one of the causes of the April 20 disaster. Halliburton said a successful test was performed on a mixture different than the one eventually used. While some tests were conducted on the new formulation requested by BP, those tests did not include a foam stability test. Halliburton made the admission in a statement responding to October 28 findings by the Presidential oil spill commission. A commission staff letter said BP and Halliburton knew weeks before the Deepwater Horizon explosion the cement mixture they planned to use to seal the new well was unstable but still completed the work.

Source: [http://www.msnbc.msn.com/id/39894210/ns/us\\_news-environment/](http://www.msnbc.msn.com/id/39894210/ns/us_news-environment/)

3. *October 29, North Andover Eagle-Tribune* – (Massachusetts) **Gasoline tanker truck fire shuts Route 93N, Massachusetts.** A gasoline tanker truck carrying about 12,000 gallons of fuel, caught fire just north of Dascomb Road on Route I-93 North in Andover, Massachusetts about 4 a.m. October 28. The fire was put out, but the vehicle remained disabled, and emergency crews were required to empty the tanker of fuel before moving it. That process required Massachusetts Highway and State Police to shut most of the highway until about 9 a.m. For a while, traffic was getting by in one lane, but when gas was being pumped from the tanker to another container, the whole highway was shut down. Brakes on the tanker had caught fire, and flames spread to the undercarriage, according to state police.

Source: <http://www.eagletribune.com/local/x2073115918/Gasoline-tanker-truck-fire-shuts-Route-93N>

4. *October 29, Torrington Register Citizen* – (Connecticut) **Crews still working to repair damage from October 28 underground electrical fire in Winsted, Connecticut.** Businesses along Main Street and some residents on Case Avenue in Winsted, Connecticut were still without power October 29 following an underground explosion and electrical fire that occurred at about 12:30 p.m. October 28. On October 29, a Connecticut Light and Power (CL&P) spokesman said crews worked through the night to repair wires damaged by the fire, and were working to get the repairs done as

quickly as possible. The fire caused Main Street to be closed in both directions from Case Avenue to Meadow Street. A short in an underground secondary electrical conductor caused the fire, according to another spokesman from CL&P. All power sources were shut off so work crews could go underground to repair the problem.

Source:

<http://www.registercitizen.com/articles/2010/10/29/news/doc4cc9d8a640840637872053.txt>

5. *October 28, v3.co.uk* – (International) **Stuxnet-like attack could hit U.S. energy grid.** The United States is bracing for an attack on its national energy grid computing systems involving Stuxnet-like malware, according to a senior director from the Department of Energy (DOE). The director of DOE's Transparency Initiative, told attendees at a conference organized by the Armed Forces Communications and Electronics Association that "it is going to happen." He said the department has already taken preventative steps, such as ensuring a high level of redundancy in the network and a defense-in-depth approach to cyber security. Stuxnet was branded "probably the most important malware in the last 10 years" by the F-Secure chief research officer at the event. The malicious code exploited four, zero-day vulnerabilities in its mission to disrupt industrial supervisory control and data acquisition systems, and is likely to have been crafted by a state-backed group. However, the director warned Stuxnet is not the only threat facing critical national infrastructures such as the U.S. energy grid, and that the utility industry's move towards smart grids could pose new security threats globally. "We had a simple point-to-point system with a clearly defined set up of controls, but as [the system] gets smarter with localized intelligence, the risk will increase," he said. "With multi-layered interconnectivity you are opening the door to a broader set of vulnerabilities."

Source: <http://www.v3.co.uk/v3/news/2272384/stuxnet-attack-hit-energy-grid>

6. *October 28, Bangor Daily News* – (Maine) **Ellsworth police look for suspects in utility pole copper wire thefts.** Police are searching for thieves who apparently used an ax to cut copper ground wires from light poles in Ellsworth, Maine. According to an Ellsworth Police officer, the wire was cut from 23 light poles along Gary Moore and Sunset Park roads sometime within the past 30 to 60 days. The time frame is based on a report from Bangor Hydro-Electric Co. of when it last inspected the poles in that area, the officer said. "Someone had used an ax or a hatchet to cut the wire. You could see the indentation in the wood," he said. The specialized wire is used primarily in commercial and industrial operations. Bangor Hydro crews are still investigating the incident and trying to determine whether any other poles in the area were targeted. The firm has to deal with this type of crime regularly, including copper thefts at substations, a company spokeswoman said.

Source: <http://www.istockanalyst.com/article/viewiStockNews/articleid/4622336>

For another story, see item [34](#)

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

## **Chemical Industry Sector**

7. *October 28, United Press International* – (National) **Flame retardants said hazardous to health.** Flame retardant chemicals found in home furniture, electronics, insulation, mattresses, and other products are hazardous, U.S. environmentalists said. Brominated and chlorinated flame retardants can cause serious health harm while providing only limited fire safety benefits, according to an October 28 release from Safer Chemicals, Healthy Families, a coalition of 250 environmental health groups. The coalition is urging an overhaul of the 1976 Toxic Substances Control Act, the current federal law regulating chemicals. During the last Congressional session, two proposals were presented to overhaul the law, but neither reached a vote. New bills are expected to be introduced in the next session.

Source: [http://www.upi.com/Science\\_News/2010/10/28/Flame-retardants-said-hazardous-to-health/UPI-99511288308859/](http://www.upi.com/Science_News/2010/10/28/Flame-retardants-said-hazardous-to-health/UPI-99511288308859/)

8. *October 28, WUPW 36 Toledo* – (Ohio) **Nitric acid spill closes turnpike lanes.** Ohio Turnpike officials closed the eastbound lanes and then the westbound lanes near Wauseon after a truck carrying upwards of 250 gallons of nitric acid started to smoke October 28. The truck was transporting nitric acid inside containers, which leaked onto the turnpike near mile marker 35, which is between Wauseon and Delta. The smoke was first reported at 3:20 p.m., after an Ohio State Highway Patrol trooper stopped the commercial semi. The turnpike commission reported on its Web site the closure spanned 7.6 miles between Milepost 28.4 to 36.0. Hazmat crews approached the rear of the commercial truck and capped the leak source. The westbound lanes were opened before 9 p.m. The eastbound lanes were opened about a half-hour later. There were no injuries and the incident remains under investigation. The semi is employed by Barr Transportation Networking out of Wilmette, Illinois.

Source: <http://www.foxtoledo.com/dpp/news/local/Nitric-acid-spill-closes-turnpike-lanes>

For another story, see item [28](#)

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

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

9. *October 29, Southern Maryland Newspapers* – (International) **New hope for third nuclear reactor.** Constellation Energy and Electricite de France (EDF) reached an agreement October 26, announcing that EDF will purchase Constellation's half of their U.S. nuclear venture, UniStar Nuclear Energy, for \$140 million — making room for EDF to potentially move forward with the loan guarantees for the third reactor at Calvert Cliffs Nuclear Power Plant in Lusby, Maryland. The agreement, according to a press release, restructures the partnership, does away with the put option that held the partnership in jeopardy, and makes EDF UniStar's sole owner. The release also makes it clear that Calvert Cliffs' third reactor, and even a possible fourth reactor, may now be in the works again: "In addition to sites for Calvert Cliffs 3 and a potential fourth

reactor at Calvert Cliffs, which are both held by UniStar, Constellation will transfer to UniStar potential nuclear sites at Nine Mile Point and R.E. Ginna in New York State.”  
Source: [http://www.somdnews.com/stories/10292010/rectop175945\\_32367.shtml](http://www.somdnews.com/stories/10292010/rectop175945_32367.shtml)

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

## **Critical Manufacturing Sector**

10. *October 28, AOL Daily Finance* – (National) **U.S. workplace injuries down 8% on manufacturing improvements.** U.S. nonfatal workplace injuries and illnesses fell about 8 percent last year, as manufacturers had the largest one-year percentage drop in such incidents in at least 6 years, the U.S. Labor Department’s Bureau of Labor Statistics (BLS) said October 28. Nonfatal workplace injuries and illnesses affected 3.6 percent of full-time workers in 2009, down from 3.9 percent in 2008, the BLS said in its report. State and local government workers had the highest incidence of injuries and illnesses, and were about three times as likely to be hurt or sick as workers in the information and financial-services fields. Declines in manufacturing-industry incidents helped pull the overall numbers down. Manufacturing illnesses and injuries dropped about 12 percent in 2009, to 4.3 percent of all full-time workers, the lowest figure since the BLS started keeping such statistics in 2003. About 30 percent of injuries and illnesses across all industries forced the affected worker to miss work days, while about 25 percent caused the employee to either change jobs or be restricted from certain activities on the job, according to the BLS.  
Source: <http://www.dailyfinance.com/story/u-s-workplace-injuries-down-8-on-manufacturing-improvements/19693975/>

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

## **Defense Industrial Base Sector**

11. *October 29, Fosters Daily Democrat* – (International) **Fire near U.S.S. Virginia quickly extinguished at shipyard.** A fire broke out at the Portsmouth Naval Shipyard in Maine at the work site of the docked USS Virginia October 27. Around 6:20 p.m. Portsmouth Naval Shipyard Fire Department officials were called to Dry Dock #3 where a ventilation blower filter had caught fire. The dry dock was supporting the non-nuclear Main Ballast Tank work for the submarine at the time. Officials were able to immediately extinguish the fire, according to the shipyard. There were no injuries and the cause of the fire is still under investigation. The 377-foot-long USS Virginia submarine is currently undergoing a 14-month overhaul at the shipyard for maintenance repairs.  
Source:  
[http://www.fosters.com/apps/pbcs.dll/article?AID=/20101029/GJNEWS\\_01/710299905/-1/fosnews](http://www.fosters.com/apps/pbcs.dll/article?AID=/20101029/GJNEWS_01/710299905/-1/fosnews)
12. *October 28, Tucson Citizen* – (National) **Mesa aviation executive indicted on arms charges.** The owner of an east Mesa, Arizona company that converts aging World War

II aircraft into firefighting air tankers has been indicted by a federal grand jury in connection with the unauthorized export of military aircraft engines to the Venezuelan Air Force. The two-count indictment alleged the CEO of Marsh Aviation Co. violated the Arms Export Control Act and engaged in a conspiracy in the export of engines designed for the OV-10 Bronco, a light armed reconnaissance aircraft suited for counter-insurgency missions. The engines are listed on the United States Munitions List, and their export is illegal without a license or written authorization from the State Department, according to the indictment returned the week of October 25 in Phoenix. The indictment also alleged the CEO and his firm furnished assistance to members of the Venezuelan Air Force, including training, in the assembly, testing, repair, maintenance, modification, operation, and use of the T-76 military aircraft engine, without the required license or written authorization from the State Department. Source: <http://tucsoncitizen.com/arizona-news/2010/10/28/mesa-aviation-executive-indicted-on-arms-charges/>

13. *October 28, Bloomberg* – (National) **Northrop Navy ships ‘not survivable’ in combat, official says.** Northrop Grumman Corp.’s \$1.68 billion amphibious warship, designed to transport Marines close to shore, would not be effective in combat and could not operate reliably after being hit by enemy fire, according to the Department of Defense’s (DOD’s) top testing official. The San Antonio-class vessel’s critical systems, such as electrical distribution, ship-wide fiber optics and voice- communications networks, are not reliable, according to the DOD’s director of operational test and evaluation. The ship’s armaments cannot effectively defend against the most modern anti-ship weapons, he said. The ship is capable of operating “in a benign environment,” he said in an e-mail to Bloomberg News outlining the unclassified summary of a classified report sent to Congress in June. The vessel is “not effective, suitable and not survivable in a combat situation,” he said. The test report is the latest black eye for a program that has faced reliability and construction questions since the first of the ships — the USS San Antonio, also called the LPD-17 — was delivered in 2005, more than 3 years behind schedule.

Source: <http://www.bloomberg.com/news/2010-10-28/northrop-navy-ships-not-survivable-in-combat-u-s-defense-official-says.html>

14. *October 28, Federal Bureau of Investigation* – (Colorado) **Army contracting officer pleads guilty in Colorado to bribery related to contracts.** A U.S. Army major pleaded guilty October 28 to a one-count criminal information charging him with bribery for accepting money and items of value in return for being influenced in the awarding of Army contracts. The man pleaded guilty in United States District Court for the District of Colorado. According to court documents, at various times from approximately 2004 through 2007, the defendant was employed by the U.S. Army and deployed overseas in Afghanistan, Iraq, and Kuwait as a contracting officer. The defendant admitted that during that time period he accepted illicit bribe payments from foreign companies seeking to secure Army contracts. In return, he used his official position to steer Army contracts to these firms. During the course of this criminal scheme, he accepted Rolex watches, cash payments, and other things of value totaling more than \$200,000. He faces a maximum prison sentence of 15 years, a fine of



\$250,000, and 5 years of supervised release following his prison term.

Source:

[http://7thspace.com/headlines/361859/army\\_contracting\\_officer\\_pleads\\_guilty\\_in\\_colorado\\_to\\_bribery\\_related\\_to\\_contracts\\_.html](http://7thspace.com/headlines/361859/army_contracting_officer_pleads_guilty_in_colorado_to_bribery_related_to_contracts_.html)

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

## **Banking and Finance Sector**

15. *October 29, MetroWest Daily News* – (Massachusetts) **Hopkinton man charged with \$30 million in fraud.** A Hopkinton, Massachusetts man has been accused of defrauding more than 1,000 customers out of more than \$30 million, authorities said. The FBI arrested the 50-year-old at his Thayer Heights home October 28. He is charged with nine counts of wire fraud, and two tax offenses. The suspect was the owner of the now-defunct Boston Trading and Research. The U.S. Justice Department (DOJ) said the company, co-owned by a partner, used customers' money in a foreign currency exchange market. The (DOJ) has issued a warrant for the other suspect's arrest, charging him with 10 counts of wire fraud. Authorities said he left for Turkey in 2009 and is still at large. In the indictment, the DOJ said the two men lied to clients about how the company's trading platform worked. They said it would automatically shut down if a customer's account lost more than about 30 percent of their investment. Customers were also told the company was paid by a percentage of profits from the trading. Instead, it is alleged that the two suspects used millions of their clients' money to pay for company's operating expenses, as well as purchasing houses, cars and jewelry, federal authorities said.

Source: <http://www.metrowestdailynews.com/news/x370073167/Hopkinton-man-charged-with-30-million-in-fraud>

16. *October 29, Raleigh News & Observer* – (North Carolina) **Suspected repeat bank robber charged in Chapel Hill case.** The man arrested the week of October 25 in a string of bank robberies across the Triangle, North Carolina area has been formally charged in another one of the 11 holdups he is suspected of committing over the past month. The 37-year-old appeared before a Wake County magistrate October 28 to be charged with common law robbery in the October 5 holdup of the BB&T on Rosemary Street in Chapel Hill. This is the eighth charge brought against the suspect, a one-time Raleigh plumber who family members said had a long-standing problem with drugs that had driven him to rob a bank in his home state of Maryland in the mid-1990s. On October 25, after being arrested in a Durham neighborhood, the suspect was charged with six counts of common law robbery and one count of attempted common law robbery. All of those cases were related to bank robberies across Wake County. Investigators were considering charges in another Wake robbery, which occurred August 10, 2009, in Raleigh.

Source: <http://www.newsobserver.com/2010/10/29/768583/suspected-repeat-bank-robber-charged.html>

17. *October 29, Associated Press* – (National) **Couple accused of running Ponzi scheme.** The FBI is seeking a husband and wife accused of running a Ponzi scheme that bilked about \$3 million from a dozen investors, nine of whom lived in Hawaii. The couple were indicted October 28 by a federal grand jury in Honolulu on 13 counts of wire and mail fraud relating to the scheme that allegedly operated from 2005 through 2009. Part of the time, the husband was incarcerated in federal prisons in Nevada, Texas, and California. While incarcerated in Nevada, he was housed with a large number of inmates from Hawaii. The indictment alleges the couple marketed their Aloha Trading investment program to inmates and their families. The FBI believes the couple may be living in Nevada, California, or Washington.  
Source: <http://www.staradvertiser.com/news/breaking/106156903.html>
18. *October 29, HedgeCo.Net* – (National) **Hedge fund manager charged again in bridge loan scheme.** A New York hedge fund manager who was arrested in North Carolina and charged with securities fraud June 2010, has been accused of stealing an additional \$690,000, according to Bloomberg. The New York State Supreme Court in Manhattan set bail at \$1 million on the new charges, the suspect also received \$1 million bail on his previous charges. The suspect, who claimed he was directly related to Belgian royalty, was accused of stealing \$6 million from high net worth and institutional investors. He has been charged by the U.S. Securities and Exchange Commission (SEC) with using a bridge-loan facility he set up in order to run a multi-million-dollar Ponzi scheme. The SEC said back in June 2010 that the investor money also was fraudulently used to pay the suspect's massive credit card bills as well as Chimay Capital's rent and payroll, and to pay off disgruntled counterparties in the suspect's other business ventures. In December 2009, the suspect sought a multi-million dollar bank loan on the basis of false representations that he had \$13 million in liquid assets in a Bermuda bank account. The account balance was actually zero.  
Source: <http://www.hedgeco.net/news/10/2010/hedge-fund-manager-chimay-charged-again-in-bridge-loan-scheme.html>
19. *October 28, WHSV 3 Harrisonburg* – (Virginia) **Three Suspects Arrested in Major Credit Card Scam.** The Augusta County Sheriff's Office in Virginia confirms that three suspects, all from New York, were arrested October 26 in connection to credit card scam that operated along the East Coast. The three suspects were taken into custody at the Verona Food Lion on Laurel Hill Road in Verona, Virginia, without incident. Numerous credit cards were seized from the suspects, according to a sheriff's office spokesperson. Officials report each suspect was charged with nine counts of credit card fraud. Additional charges may be pending. The suspects are being held at the Middle River Regional Jail.  
Source:  
[http://www.whsv.com/news/headlines/Three\\_SuspectsArrested\\_In\\_Major\\_Credit\\_Card\\_Scam\\_105878538.html](http://www.whsv.com/news/headlines/Three_SuspectsArrested_In_Major_Credit_Card_Scam_105878538.html)
20. *October 27, IDG News Service* – (National) **Fraudsters find holes in debit card fraud detection.** Over the last few weeks, criminals have been exploiting weak fraud detection systems used for debit cards with "flash" attacks, where hundreds of



withdrawals are made over a very short period of time. Banking executives have noticed a rise in such attacks, where fraudsters withdraw money throughout a wide region within minutes, said a Gartner vice president, who frequently consults with banks about fraud issues. “The fraud happens within 10 minutes in these geographic diverse locations,” she said. The amounts withdrawn are usually within a range that would not immediately raise a red flag, the vice president said. She said a Canadian banker she spoke with noticed withdrawals from 100 ATMs all over Canada within 10 minutes. The pattern shows the criminal gangs are clearly coordinating the timing of the withdrawals using money mules, or people who are hired to do the risky job of taking fraudulent payment cards to ATMs that are often under video surveillance. The fraudsters seem to be targeting debit cards, which have less sophisticated fraud detection systems in place than credit cards, the vice president said. Credit card systems are more likely to catch anomalies such as when a person uses a card in New York, and then just hours later a transaction with the same card shows up in California.

Source:

[http://www.computerworld.com/s/article/9193378/Fraudsters\\_find\\_holes\\_in\\_debit\\_card\\_fraud\\_detection](http://www.computerworld.com/s/article/9193378/Fraudsters_find_holes_in_debit_card_fraud_detection)

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

## **Transportation Sector**

21. *October 29, CNN* – (International) **U.S. alert focuses on cargo after suspicious packages found overseas.** Suspicious packages found in at least two locations abroad that were on planes bound for the United States “apparently contain explosive material,” the U.S. President said late in the afternoon October 29, calling the discovery “a credible threat against our country.” The packages led to increased searches of cargo planes and trucks in several U.S. cities, said law enforcement sources with detailed knowledge of the investigation. U.S. officials believe that al Qaeda in the Arabian Peninsula, commonly referred to as AQAP, is behind the incident. The President confirmed that the packages originated in Yemen — the stronghold of al Qaeda in the Arabian Peninsula. “We also know that al Qaeda in the Arabian Peninsula continues to plan attacks against our homeland, our citizens, and our friends and allies,” he said during a press briefing on the incident. One suspicious package found in the United Kingdom contained a “manipulated” toner cartridge and had white powder on it as well as wires and a circuit board, a law enforcement source said. A similar package was discovered in Dubai, in the United Arab Emirates, the source said. Both packages were bound for the United States, “specifically two places of Jewish worship in Chicago,” the President said. Authorities were looking for about 13 other packages shipped from Yemen, a law enforcement source said. The plot could be a dry run to test Western security, another U.S. official told CNN. The furor led to heightened inspection of arriving cargo flights in Newark, New Jersey, and Philadelphia, Pennsylvania, and a UPS truck in New York.

Source:

<http://www.cnn.com/2010/US/10/29/security.concern/index.html?hpt=T1&ieref=BN1>

22. *October 29, Washington Post* – (District of Columbia; Maryland; Virginia) **Suspect in Metro plot aspired to kill troops abroad, FBI says.** The man charged in an alleged plot to blow up Washington Metropolitan Area Transit Authority (Metro) rail stations in Northern Virginia suggested ways to kill as many people as possible on the subway, wanted to battle U.S. troops in Afghanistan and Pakistan, and trained himself to fight, authorities alleged October 27. The Ashburn, Virginia man never suggested any attacks inside the United States, and the plot to attack Metro was hatched by government operatives posing as terrorists, according to court records unsealed October 28. The man told undercover FBI operatives who he thought were al-Qaeda terrorists that he was ready to martyr himself in battle, according to government documents.  
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/10/28/AR2010102807326.html>
23. *October 29, Associated Press* – (Florida) **Hole found in plane that took off from Miami.** Authorities said a 1-foot-by-2-foot hole was found in the fuselage of a commercial airliner that suddenly lost cabin pressure shortly after taking off from Miami, Florida. A Federal Aviation Administration spokeswoman said oxygen masks were deployed when American Airlines Flight 1640 lost cabin pressure about 30 minutes into its flight October 26. The Boeing 757 carrying 154 passengers and six crew members had left Miami for Boston, Massachusetts. An inspection of the plane revealed a 1-foot-by-2-foot hole in the upper part of the fuselage near a cabin door toward the front of the plane. American Airlines said the crew declared an emergency and returned safely to Miami.  
Source: <http://www.miamiherald.com/2010/10/29/1897732/hole-found-in-plane-that-took.html>
24. *October 29, New York Times* – (International) **Cargo planes checked for suspicious packages.** Federal investigators swept cargo planes at two United States airports October 29, searching for suspicious packages, after a potentially explosive device was found October 28 at an airport near Birmingham, England, originating in Yemen and bound for Chicago. Officials isolated UPS cargo planes that landed at Philadelphia and Newark airports on Friday morning because they were carrying packages that appeared to have the same origin as the suspicious device in Britain. A UPS truck in Brooklyn was also stopped and checked on Friday. But in each case, the packages that reached the United States have been found to be nonthreatening. At East Midlands Airport in Britain, where UPS has a cargo sorting facility, the attention of security officials was attracted to a suspicious package that had come from Yemen. They found in it a toner cartridge that appeared to have been tampered with in a way that made it resemble an improvised bomb, though tests for the presence of explosives were negative, a law enforcement official said.  
Source: <http://www.nytimes.com/2010/10/30/us/30plane.html?hp>
25. *October 28, Washington Post* – (District of Columbia; Maryland; Virginia) **Survey: Most Metro workers see safety violations, many do nothing about it.** Only 10 percent of Washington Metropolitan Area Transit Authority (Metro) employees said they had not witnessed a safety breach in the past year, according to an unprecedented

safety survey of the Washington D.C. transit system completed in July 2010 by more than 9,300 workers. Almost 30 percent said they did not know if they had witnessed a safety breach. The survey was part of an effort to gauge Metro's "safety culture." Federal investigators probing the June 2009 Red Line crash said Metro's negligent attitude toward safety contributed to the accident. According to the summary, the survey found that more than 30 percent of the Metro workers who had observed safety violations in the past year failed to report the problems, because they feared retaliation or doubted that Metro would fix them. The most common safety problem — identified by nearly 40 percent of respondents — was unsafe working conditions. Survey respondents reported widespread texting and cellphone use by employees operating Metro's trains, buses and other vehicles. Metro instituted a zero-tolerance policy last year; requiring the dismissal of bus and train operators for first offenses.

Source: [http://www.washingtonpost.com/wp-dyn/content/article/2010/10/28/AR2010102807214.html?wprss=rss\\_metro](http://www.washingtonpost.com/wp-dyn/content/article/2010/10/28/AR2010102807214.html?wprss=rss_metro)

26. *October 28, Los Angeles Times* – (International) **4 killed in bus attacks in northern Mexico.** Armed men opened fire on buses carrying assembly plant workers near the Texas border October 28, killing four people and wounding 15 others in the latest spasm of violence to rattle Mexico. Authorities in the northern state of Chihuahua said the victims, identified as employees of a U.S. car-upholstery plant called Eagle Ottawa, were riding home about 1 a.m. when three company buses came under fire outside Ciudad Juarez. Witnesses said gunmen jumped aboard looking for a male passenger. Source: <http://www.kentucky.com/2010/10/28/1499457/4-killed-in-bus-attacks-in-northern.html>

For more stories, see items [3](#) and [8](#)

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

## **Postal and Shipping Sector**

27. *October 29, Federal Bureau of Investigation* – (Alabama) **Alabama man charged with mailing hoax Anthrax letters.** A federal grand jury today indicted a Madison County, Alabama man for mailing hoax anthrax letters in September 2010 to political offices in Homewood, Alabama and Washington, D.C., and to an insurance office in Nebraska, the U.S. district attorney and U.S. Postal Inspector announced October 28. In a three-count indictment filed in United States District Court, the grand jury charges the 71 year-old suspect with mailing letters containing a powdery substance to the Alabama Republican Party office in Homewood, the Center for Responsive Politics in Washington, D.C., and the Mutual of Omaha Insurance Company in Omaha, Nebraska. Each envelope included a typewritten note referring to the mailing as a "Koran Puffie," according to court records. Testing of the substance found in all three letters was negative for the presence of anthrax or any other biological hazard. Source: [http://7thspace.com/headlines/361860/alabama\\_man\\_charged\\_with\\_mailing\\_hoax\\_anthrax\\_letters\\_.html](http://7thspace.com/headlines/361860/alabama_man_charged_with_mailing_hoax_anthrax_letters_.html)

## **Agriculture and Food Sector**

28. *October 29, St. Petersburg Times* – (Florida) **Hazmat crews respond to ammonia leak at empty St. Petersburg warehouse.** Hazardous materials crews responded October 28 to an ammonia leak at an empty seafood warehouse in St. Petersburg, Florida. The incident began about 1:30 p.m. as firefighters with St. Petersburg Fire Rescue were doing a routine hazardous materials inspection at 333 16th Ave. S, a department spokesman said. The building houses a processing facility for Key West Fresh and Frozen Seafood. When crews got there, the door was open and there was a strong odor of anhydrous ammonia. Hazardous materials firefighters began searching the building and found a 14-gallon ammonia tank with about 5 gallons left in it, and an apparent small leak at the valve. A total of 27 hazmat technicians from St. Petersburg, Largo, Pinellas Park, Palm Harbor, and Seminole responded. The leak was limited to the building, and though several streets were closed, surrounding buildings were not evacuated. A Key West Fresh representative told fire officials the company has not been in the building for 2 months.

Source: <http://www.tampabay.com/news/publicsafety/hazmat-crews-respond-to-ammonia-leak-at-empty-st-petersburg-warehouse/1130843>

29. *October 29, Associated Press* – (California) **Toxic acid found in parts of California lobster, crab.** State officials are warning fans of California spiny lobster and rock crab to eat only the tail meat and not internal organs after finding a toxic acid in samples. The department of fish and game said October 28 the warning applies to all lobster and rock crab harvested in Southern California until further notice. Investigators found high levels of domoic acid in lobsters and crabs around the northern Channel Islands. Poisoning can occur 30 minutes to 24 hours after consumption. Symptoms range from nausea, diarrhea, cramps, headache, and dizziness, but in severe cases can be life-threatening. Domoic acid is found in the marine algae consumed by small fish, clams, and mussels, which are in turn eaten by crustaceans, resulting in a concentration of acid in their organs.

Source: <http://www.foxnews.com/health/2010/10/29/toxic-acid-parts-california-lobster-crab/>

30. *October 28, Associated Press* – (Tennessee) **Cotton modules burn in Dyer County, Tenn., fire likely set.** A fire that officials call suspicious has destroyed 96 cotton modules in Dyersburg, Tennessee. The State Gazette reported Dyer County Fire Department firefighters were dispatched to the Chic community near the Mississippi River October 26. The compacted cotton is difficult to extinguish, and firefighters could do little but keep the flames from spreading. The cotton farmer estimated the modules — each of which contains 4-5 bales of cotton — were worth about \$160,000. He said his crop was insured.

Source:

[http://wdef.com/news/cotton\\_modules\\_burn\\_in\\_dyer\\_county\\_tenn\\_fire\\_likely\\_set/10/2010](http://wdef.com/news/cotton_modules_burn_in_dyer_county_tenn_fire_likely_set/10/2010)

31. *October 28, Food Poison Journal* – (National) **Two different sets of pork products recalled for Listeria.** Two corporations are recalling pork products due to listeria concerns. To this point, neither recall has been linked to reported illnesses. Valley Farm Meats, also known as Strasburg Provision, of Wooster, Ohio is recalling 3,600 pounds of (primarily) pork products. Autentico Foods of California is recalling 54,000 pounds of pork. The recalled Valley Farm products may bear the Ohio Department of Agriculture inspection mark and the Establishment mark, “Est. 80.” The products were produced this year between June 1 and October 4. The Autentico Foods recall second recall was announced by the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS). The recalled pork products bear an establishment mark “Est. 3810.” The products were sent to retailers in California, Colorado, Florida, Idaho, Nevada, New York, Oklahoma, Texas, and Utah.  
Source: <http://www.foodpoisonjournal.com/2010/10/articles/food-poisoning-watch/two-different-sets-of-pork-products-recalled-for-listeria/>
32. *October 28, Associated Press* – (Minnesota) **7 more sickened after drinking raw milk in Minn.** Illnesses in seven more people have been tied by to the consumption of raw milk from a farm in Sibley County, Minnesota, that was implicated in an E. coli outbreak earlier in 2010, the Minnesota Department of Health reported October 28. Three people were infected with a bacterium called campylobacter jejuni and the other four with a parasite, cryptosporidium parvum, after drinking raw milk. All seven reported drinking raw milk, and those who named a source said it was the Hartmann Dairy Farm, the department said. Laboratory tests determined the bacterium and parasite in most of the ill people were genetically identical to samples taken from the farm this summer. Both result in similar symptoms, including fever, diarrhea and vomiting. Cryptosporidium can be life threatening for people with weak immune systems. The seven people were sickened from late July to late August.  
Source: <http://www.businessweek.com/ap/financialnews/D9J4UMJO0.htm>
33. *October 28, Associated Press* – (Wyoming) **Possible brucellosis case in Park Co., Wyo., cows.** Preliminary tests indicated the bacterial disease brucellosis has been found in three cows in northern Wyoming. The Wyoming Livestock Board said more tests are being done to confirm the disease in the cows from a single herd in Park County. Nearby herds also are being tested. Results could take about 2 weeks. Brucellosis is a bacterial disease that can cause pregnant bison, cattle, and elk to abort their fetuses. Strict measures are taken if it spreads to cattle in order to protect the beef industry. Wyoming last had a confirmed case of brucellosis in cattle just over 2 years ago in Sublette County.  
Source: <http://www.farmforum.net/node/24265>

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

## **Water Sector**

34. *October 29, Fort Collins Coloradoan* – (Colorado) **Oil regulators seek water tests.** Colorado oil and gas regulators are asking energy companies drilling in northern

Weld and Larimer counties to test the groundwater before they start producing oil so the state can find out how energy development may contaminate the groundwater in the region. The tests, which will establish a baseline for water quality where oil and gas companies are rushing to buy up mineral leases so they can drill the potentially oil-rich Niobrara Formation, are a protective measure required in southern Weld County but not yet in Northern Colorado. “It’s an area where we don’t have a lot of baseline information at this time, and where we are anticipating significant oil and gas development in the future,” said the Colorado Oil and Gas Conservation Commission director. The information will help the state respond to residents’ complaints about suspected domestic water well contamination from nearby oil and gas development, he said.

Source: <http://www.coloradoan.com/article/20101029/NEWS01/10290315>

35. *October 28, Associated Press* – (Oregon) **Broken water main floods homes in Bend, Ore.** A water main break in downtown Bend, Oregon, shot water 70 feet into the air, flooding several homes. City officials said that a 12-inch water main broke near Riverside Boulevard and Kansas Avenue around 3:15 a.m. October 28, flooding the area with about 2,000 to 3,000 gallons per minute. Streets around the break were closed as city crews worked in knee-deep water to stop the flow — an effort that took about 1 hour. The garage at one home caved in and a tree was split apart. Most of the water receded by 7 a.m., leaving behind a big mess for residents to clean up.

Source: [http://democratherald.com/news/state-and-regional/article\\_53de4567-9d78-5664-b0e8-b365f1c57057.html](http://democratherald.com/news/state-and-regional/article_53de4567-9d78-5664-b0e8-b365f1c57057.html)

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

## **Public Health and Healthcare Sector**

36. *October 28, Computerworld* – (California) **IT worker gets prison after stealing data for online surveys.** A former IT staffer was sentenced October 27 to 1 year and 1 day in prison for stealing sensitive information belonging to his co-workers and using the data to make money filling out online health surveys. The man was fired from the University of California San Francisco (UCSF) Medical Center earlier this year after investigators discovered that he had used the names, birthdays, and Social Security numbers of other UCSF employees to fill out 382 online surveys in order to collect online vouchers, worth \$100 each. He had worked at the medical center’s IT department for 5 years and had access to the sensitive information through his job, according to court records. In court filings, the man’s attorney said he received 218 vouchers (total value \$21,800) but never managed to cash them in. He only used part of the Social Security numbers of his co-workers while filling out the survey, his lawyer said. The man pleaded guilty to wire fraud and identity theft charges July 22. He was sentenced in the U.S. District Court for the Northern District of California.

Source:

[http://www.computerworld.com/s/article/9193818/IT\\_worker\\_gets\\_prison\\_after\\_stealing\\_data\\_for\\_online\\_surveys?taxonomyId=17](http://www.computerworld.com/s/article/9193818/IT_worker_gets_prison_after_stealing_data_for_online_surveys?taxonomyId=17)



37. *October 27, Federal Bureau of Investigation* – (Texas) **Marketer indicted for health care fraud.** A nine-count sealed indictment charging a Houston, Texas, man with conspiracy to commit health care fraud and health care fraud has been unsealed, a United States Attorney and the Texas Attorney General announced October 27. The charges arise from a scheme to defraud Medicare of more than \$2.76 million. In the 3-year scheme the man allegedly provided Medicare beneficiaries' information — including names, addresses, and Medicare numbers — to file false claims purportedly for arthritis kits to Sefan Health Care Services Inc. The investigation is part of the Medicare Fraud Strike Force, and was the result of a joint investigation by agents of the Department of Health and Human Services, Drug Enforcement Administration Diversion Division, Texas Attorney General Medicaid Fraud Control Unit, United States Railroad Retirement Board, and the FBI.  
Source: <http://houston.fbi.gov/dojpressrel/pressrel10/ho102710.htm>

38. *October 26, Associated Press* – (International) **GlaxoSmithKline settles bad drug case for \$750M.** British pharmaceutical company GlaxoSmithKline PLC will pay \$750 million to settle allegations it knowingly manufactured and sold adulterated drugs, including the popular antidepressant Paxil, federal prosecutors in Massachusetts said October 26. A U.S. Attorney announced that the London-based company will pay \$150 million in criminal fines and \$600 million in civil penalties related to faulty manufacturing processes at its plant in Cidra, Puerto Rico. The company allowed several drugs to be adulterated between 2001 and 2005, including Paxil CR, a skin-infection ointment called Bactroban, an anti-nausea drug called Kytril, and a diabetes drug called Avandamet, the attorney said. The \$600 million civil penalty will be paid to the federal government and the states to cover false claims submitted to the Medicaid program and other health care programs.  
Source:  
[http://www.boston.com/business/healthcare/articles/2010/10/26/glaxosmithkline\\_to\\_pay\\_750\\_million\\_in\\_pill\\_case/](http://www.boston.com/business/healthcare/articles/2010/10/26/glaxosmithkline_to_pay_750_million_in_pill_case/)

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

## **Government Facilities Sector**

39. *October 29, CNN* – (Virginia) **Shots fired at Marine Corps museum in suburban Washington.** Several shots were fired at the National Museum of the Marine Corps building in Triangle, Virginia, the FBI said October 29. No injuries were reported. It is the second time the Marine Corps museum has been fired upon in recent days. In addition, the Pentagon and a vacant Marine Corps Recruiting Station in Virginia also were shot at recently. All the previous shots came from the same weapon, authorities said. The latest incident occurred October 28, a spokeswoman at the National Museum of the Marine Corps said, noting no one was in the building at the time. Bullet holes were found in the glass and metal structure of the building but not inside, she said. The museum was closed early October 29 while the investigation continued, the spokeswoman said, adding it would remain closed the rest of the day.

Source:

<http://www.cnn.com/2010/US/10/29/marine.museum.shooting/index.html?hpt=T2>

40. *October 29, Associated Press* – (Hawaii) **University posts info of 40K students.** The Social Security numbers, grades and other personal information of more than 40,000 former University of Hawaii students were posted online for nearly 1 year before being removed the week of October 25, the Associated Press (AP) has learned. University officials told AP that a faculty member inadvertently uploaded files containing the information to an unprotected server November 30, 2009, exposing the names, academic performance, disabilities, and other sensitive data of 40,101 students who attended the flagship Manoa campus from 1990 to 1998, and in 2001. A handful of students from the West Oahu campus were included in the security breach. A UH-West Oahu spokesman said there was no evidence the faculty member acted maliciously or that any of the data was used improperly.

Source: <http://www.kivitv.com/Global/story.asp?S=13408038>

41. *October 29, Altoona Mirror* – (Pennsylvania) **Fires force football team's evacuation.** The Altoona Area Junior High White football team was forced to evacuate Gus Anderson Field during its game October 28 with Erie McDowell as four fires and a suspicious device were discovered at the nearby McDowell Senior High School in Erie, Pennsylvania. One juvenile was in custody, the Erie Times-News reported on its Web site. All students and personnel were evacuated from the school after a fire was reported about 3:15 p.m., the Millcreek Township School District said on its Web site. Three other fires were reported in the school, with damage to the basement, a locker room, the auditorium stage, and another room. After the suspicious device was discovered, McDowell's athletic director was told to stop the football game, an Altoona Area School District spokesman said. The suspicious device thought to be a bomb turned out to be a radio wrapped in wire, the Erie newspaper reported.

Source: <http://www.altoonamirror.com/page/content.detail/id/543740/Fires-force-football-team-s-evacuation.html?nav=742>

42. *October 28, Lompoc Record* – (California) **Update: Fire on Vandenberg AFB prompts evacuation, beach closure.** A wind-driven fire that quickly swelled to 400 acres October 28 prompted partial evacuation of south Vandenberg Air Force Base in Lompoc, California and the precautionary closure of Surf Beach as officials hope for the quick arrival of rainy weather. Base officials asked the public to stay away to avoid interfering with emergency personnel. "We're trying to put the fire in a box," using containment lines and fire breaks such as roads, said Santa Barbara County Fire Department captain. "We'll be working to contain the fire with the hope that we get rain, and the winds die down," said a Vandenberg spokeswoman. Crews battling the flames also had to deal with an unusual danger — some areas have unexploded ordnance left over from the area's use as an Army training facility. That has dictated how they work to control the fire, officials said. Additionally, several power poles have been burned by the flames. Dubbed the Bear Creek Fire, because it's burning south of Bear Creek Road, the blaze started in heavy brush that, paired with warm temperatures and high winds, quickly fueled the flames.

Source: [http://www.lompocrecord.com/news/local/article\\_ac9a75c0-e2d2-11df-b814-001cc4c03286.html](http://www.lompocrecord.com/news/local/article_ac9a75c0-e2d2-11df-b814-001cc4c03286.html)

43. *October 28, Federal Computer Week* – (National) **NARA shows gaps in cybersecurity, GAO says.** The National Archives and Record Administration (NARA) should improve its cybersecurity programs and use better management to safeguard official records, according to two new reports from the Government Accountability Office (GAO). NARA is in charge of preserving official documents and electronic records from federal agencies. Its workload is growing, as holdings requiring preservation grew from about 2.4 million cubic feet in 2008 to about 2.6 million cubic feet in 2009, not including digital documents, GAO said. However, the agency has gaps in achieving its goals, due to shortcomings in cybersecurity and management, the GAO said in two reports, both released October 27. In the cybersecurity report, GAO said NARA has not deployed sufficient information security controls to ensure the integrity of the data it stores. Despite use of encryption, access controls and other protections, there were gaps related to policies and procedures, including inconsistent network monitoring, spotty user authentication, weak access controls and deficient physical security, among other problems, the report states. Overall, there were 142 weaknesses identified in the audit.

Source: <http://fcw.com/articles/2010/10/28/nara-archives-cybersecurity.aspx>

44. *October 28, Associated Press* – (National) **US cyber officer says nation isn't in a cyberwar, but networks are being contested.** A military commander said the United States is not in a cyberwar, but critical networks are being “contested” and the threat of any deliberate or accidental disaster is formidable. An Air Force major general and chief of staff of U.S. Cyber Command did not identify who is contesting U.S. networks, or detail the nature of any deliberate threats. He spoke October 28 at a homeland security symposium in Colorado Springs, Colorado. He said talk of cyberwar has been exaggerated but he said mistakes or deliberate attacks could create havoc on financial, utility, and transportation computer networks. He said dozens of people were killed in Siberia in 2009 and a hydroelectric turbine was destroyed because remote operators typed in the wrong computer commands.

Source: <http://www.kdvr.com/news/sns-ap-co--cybersecurity,0,2900945.story>

45. *October 25, NextGov* – (National) **Security flaws found in systems that track recovery-related spending at Transportation.** Transportation Department (DOT) Web sites that post stimulus spending results could be vulnerable to hackers looking to attack visitors' computers and manipulate data, according to the department's inspector general. In December 2009, the IG's office began examining safeguards for the systems that track the \$48 billion Congress authorized DOT to spend on projects that create jobs, such as high-speed rail and road widening. The Recovery Act requires agencies to update the public on stimulus spending via Recovery.gov, but most agencies also maintain in-house Web sites for financial management and more granular reporting. The IG published its findings on DOT sites in a report released October 25. The report uncovered 1,759 high-risk threats DOT sites. Recovery-related databases and servers also were vulnerable to attack, but at a lower risk. The threats existed because DOT

failed to configure its sites, databases and servers according to standard controls, the audit said.

Source: [http://www.nextgov.com/nextgov/ng\\_20101025\\_4971.php](http://www.nextgov.com/nextgov/ng_20101025_4971.php)

46. *October 23, The Register* – (International; National) **Wikileaks outs 400,000 classified Iraq War docs.** Wikileaks has released almost 400,000 classified US. military documents involving the Iraq War, defying warnings from the U.S. government that disclosing the documents would put lives at risk. Dubbed “the Iraq War Logs.” the documents were posted to the whistleblower site October 22, after they were released to various news organizations across the globe. According to the The Guardian, the documents show U.S. commanders ignored evidence of torture by Iraqi police and soldiers, and that more than 15,000 civilians died in incidents not previously reported. Though U.S. officials have said they kept no official record of civilian deaths, the leaked documents show that 66,081 civilian died among a total of 109,000 war fatalities, according to The Guardian. It is believed the documents came from the same source that leaked 92,000 classified documents involving the Afghan war to Wikileaks earlier in 2010.

Source:

[http://www.theregister.co.uk/2010/10/23/wikileaks\\_releases\\_four\\_hundred\\_thousand\\_iraq\\_war\\_docs/](http://www.theregister.co.uk/2010/10/23/wikileaks_releases_four_hundred_thousand_iraq_war_docs/)

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

## **Emergency Services Sector**

47. *October 29, AccessNorthGA* – (Georgia) **Safety device tampering caused deputy’s car explosion.** Authorities now say the reason a Jackson County, Georgia, deputy’s car caught fire October 25 was because someone tampered with a safety device on the propane-powered cruiser. The car, being driven by a Jackson County deputy, burst into flames when he lit a cigarette as he responded to a call in Jefferson. The deputy escaped with only minor injuries. A Jackson County Sheriff’s Department major said they believe this was an isolated incident. He said the department will continue to use their propane-powered fleet. In a statement, the sheriff’s department said there were two reasons the gas entered the vehicle: “First, there had been manual tampering with the propane gas system, specifically, the safety device that prevents the discharge of propane into the vehicle’s interior was removed and disabled by an operator of the vehicle; and second, there had been improper manipulation of a fitting intended for use during maintenance procedures.” All 62 propane-powered cruisers have been grounded until they have all been inspected for safety purposes. Authorities are still unsure of who tampered with the device, and whether or not that tampering was done unknowingly or on purpose.

Source: <http://www.accessnorthga.com/detail.php?n=233376>

48. *October 29, Colorado Springs Gazette* – (Colorado) **Phone service back online in Teller County.** Phone service has been restored to Teller County, Colorado, after a major outage affected 911 service and left many land-line and cellular telephones

useless. Services went back online October 29, a dispatcher in the Teller County Sheriff's Office said. The cause of the outage was not available. The outage started October 28 and was still affecting Teller County as of 2:15 a.m. October 29, according to dispatch. Calls from working land lines were diverted to the Colorado Springs 911 call center, though people with cell phones had to contact agencies directly. Crews determined a Quest T1 line was cut, however the location has not been determined. Some Verizon lines were also tied into that severed T1 line, cutting service for both providers. Phone lines for the Cripple Creek police and fire departments were completely down, so people there were asked to call the Teller County Sheriff's Office. Source: <http://www.gazette.com/articles/county-107131-teller-service.html>

49. *October 29, New Richmond News* – (Wisconsin) **'Hams' test county's communications.** The backup emergency communication skills of area amateur radio operators, often called "hams," were recently tested in St. Croix County, Wisconsin. Amateur Radio operators conducted their annual Simulated Emergency Test in cooperation with state and local officials. Using emergency powered radios and working with local agencies, the hams had only a few hours to create extensive radio communications networks which could be used should there be a failure or overload of normal services. In addition, the ham radio operators provide "interoperability" — they can pass information between the many government and volunteer agencies which are needed in disasters but often have incompatible communication systems. This year, the St. Croix County Amateur Radio operators participated in a drill that simulated a power outage across the entire northern half of Wisconsin. They worked with the St. Croix County Emergency Operations Center, New Richmond's Westfields Hospital, and the River Falls Area Hospital to simulate supplemental communications for systems that would potentially be affected by a power outage. Source: <http://www.newrichmond-news.com/event/article/id/30801/>

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

## **Information Technology Sector**

50. *October 29, Infosecurity* – (International) **CSI 2010: Panda Labs analyst labels Mariposa masterminds as 'cyber idiots'.** While detailing Panda Security's role in taking down the Mariposa botnet, a threat analyst said the crew were hardly criminal masterminds, characterizing their technical skills as somewhat rudimentary. The Panda researcher delivered these comments during his CSI Conference session designed to glean lessons from the Mariposa botnet, whose primary operators were based in Spain, just a short train ride from the company's labs. Mariposa, Spanish for butterfly, was one of the largest known botnets at the time of its takedown according to the analyst, with more than 13 million unique IP addresses. After authorities seized equipment related to controlling the botnet, the analyst noted that the "cybercriminal was dumb enough to store all of the information unencrypted on his [personal] hard drive", which made the forensic analysis quite simple. It provided an easy-to-follow roadmap of the crime, including the names of money mules, money transfers, and so on. What the researchers also found were stolen credentials on more than 1 million people, such as

banking information, Internet log-ins, and credit card numbers. He also said that over half of Fortune 1000 companies were infected by the Mariposa botnet.

Source: <http://www.infosecurity-us.com/view/13595/csi-2010-panda-labs-analyst-labels-mariposa-masterminds-as-cyber-idots/>

51. *October 29, CNET* – (International) **Hacker shows iOS 4.2 beta for iPad jailbreak.** Jailbreaker “iH8sn0w” has released images of an iPad running the MobileTerminal jailbreak application, exposing the command line to users, suggesting that the iOS 4.2 firmware (still in beta) will be jailbroken upon its release November 2010. Fifteen-year-old hacker iH8sn0w is a proven resource in the jailbreaking world, responsible for Sn0wbreeze, iReb, iDetector, and f0recast.  
Source: <http://asia.cnet.com/crave/2010/10/29/hacker-shows-ios-4-2-beta-for-ipad-jailbreak/>
52. *October 28, Computerworld* – (International) **Hackers exploit newest Flash zero-day bug.** On October 28, Adobe confirmed hackers are exploiting a critical unpatched bug in Flash Player, and promised to patch the vulnerability in 2 weeks. The company issued a security advisory that also named Adobe Reader and Acrobat as vulnerable. “There are reports that this vulnerability is being actively exploited in the wild against Adobe Reader and Acrobat,” said Adobe in its warning. The company said it has seen no sign hackers are also targeting Flash Player itself. Those reports came from an independent security researcher who notified Adobe after spotting and then analyzing a malicious PDF file. According to the researcher, the rigged PDF document exploits the Flash bug in Reader, then drops a Trojan and other malware on the victimized machine. Adobe said all versions of Flash on Windows, Mac, Linux, and Android harbored the bug, and that the “Authplay” component of Reader and Acrobat 9.x and earlier also contained the flaw. Authplay is the interpreter that renders Flash content embedded within PDF files. Adobe promised to issue a fix for Flash by November 9, and updates for Reader and Acrobat the following week.  
Source:  
[http://www.computerworld.com/s/article/9193678/Hackers\\_exploit\\_newest\\_Flash\\_zero\\_day\\_bug](http://www.computerworld.com/s/article/9193678/Hackers_exploit_newest_Flash_zero_day_bug)
53. *October 28, techweb.com* – (International) **MS Windows can still be hacked via DLL.** According to a security advisory by ACROS Security, Microsoft’s OS Windows is still vulnerable to DLL hacking. When loading a fake DLL file, hackers can use the user’s access to post codes. The only application to prevent hackers from hiding malicious DLL files is SetDllDirectory. However, this application does not guarantee 100 percent security, as it works erratically on most of the currently used Windows versions.  
Source: <http://www.shortnews.com/start.cfm?id=86041>

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



## 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

54. *October 29, Top News* – (National) **266 Orcon customers lose their emails due to.** Internet Service Provider (ISP) Orcon, which recently experienced an “e-mail outage”, has reportedly lost the e-mails of 266 of its customers. The lost e-mails have apparently been deleted as a result of the outage. Acknowledging the fact the company experienced an e-mail outage overnight, Orcon said in an October 29 Twitter statement: “Unfortunately the outage resulted in 266 accounts losing their emails. Our engineers here are working hard to retrieve this mail; however efforts have been unsuccessful so far.” In addition, Orcon said the e-mail accounts of its remaining 200,000 customers remained unaffected by the glitch. According to reports, Orcon has informed affected customers that e-mails they have lost due to the glitch will not be restored. The recent outage at Orcon is not the first glitch reported by the ISP this month. On October 5, the company had to cope with a major outage.  
Source: <http://topnews.us/content/228232-266-orcon-customers-lose-their-emails-due-email-outage>

55. *October 29, Texarkana Gazette* – (Arkansas) **Cut cable disrupts Internet, phone service.** A severed fiber-optic cable left many De Queen, Arkansas-area residents without Internet and phone service most of the morning of October 28. Workers in a rock quarry about 3 miles west of Lockesburg accidentally cut the cable about 8:30 a.m., said a Windstream spokesman. The outage affected 5,500 to 6,000 customers in De Queen, Horatio, Wickes, and nearby communities. Cell phones, long-distance calling and DSL were disrupted. Land-line calls within the area could still be completed, he said.  
Source: <http://www.texarkanagazette.com/news/localnews/2010/10/29/cut-cable-disrupts-internet-phone-servic-72.php>

For another story, see item [48](#)

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

### Commercial Facilities Sector

56. *October 29, Associated Press* – (Nevada) **Gunman opens fire in Reno Walmart, injures 3.** A gunman was holed up October 29 at a Walmart in Reno, Nevada, after

three employees were shot and hospitalized with non-life threatening injuries, police said. About 100 people in the store were safely evacuated, police said. The lone gunman entered the store about 8:30 a.m. and started shooting in the direction of an employee or employees, the Reno deputy police chief said. “To our knowledge, he’s the only one in the store,” he told The Associated Press. “We don’t know anything about the gunman yet or his motives.” Police believe the gunman was in a back room. The deputy police chief said they were trying to contact him, but there was no dialogue so far. Employees were placed on a bus in the parking lot of a sporting goods store next to the Walmart. Washoe County deputies, Sparks police, and the FBI joined Reno police in sweeping the store to be sure there were no hostages.

Source:

<http://www.google.com/hostednews/ap/article/ALeqM5jaRcGfdb6w0qmquVprS9JYRLT9Hg?docId=9f933ea28d1e424ab7e6d0ed61a26ccc>

57. *October 28, KABC 7 Los Angeles* – (California) **Guests evacuate after Los Angeles hotel fire.** A fire broke out around 1 a.m. October 28 at the Mayfair Hotel in Los Angeles, California, on the 1200 block of West Seventh Street. The Mayfair Hotel is a 15-story residential hotel, so there were dozens of tenants and guests who had to evacuate. Firefighters knocked down the fire quickly. The blaze burned in a ballroom on the third floor of the hotel. Fire officials said a broken riser pipe that carried water to the upper floors and the sprinkler system sent a lot of water cascading down the stairwells and into at least one elevator shaft. Parts of the 84-year-old building will need to be replaced. Los Angeles City Fire Department officials said people who were staying on the lower floors should be relocated into some of the vacant rooms in the upper floors. No one was hurt, and the cause of the fire remained under investigation.

Source:

[http://abclocal.go.com/kabc/story?section=news/local/los\\_angeles&id=7751362](http://abclocal.go.com/kabc/story?section=news/local/los_angeles&id=7751362)

For more stories, see items [4](#), [27](#), and [42](#)

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

## **National Monuments and Icons Sector**

58. *October 29, Lexington Herald-Leader* – (Kentucky) **Red River Gorge fire spreads to 400 acres.** A campfire started October 23 in Red River Gorge in Kentucky during a burn ban has spread to more than 400 acres and is still burning. The U.S. Forest Service closed Tunnel Ridge Road, a part of Ky. 77 and all of the Auxier Ridge area, according to a news release from the Forest Service. The fire burned trees near the base, causing them to fall and block the roadway. The highway is closed from Nada Tunnel to the Martins Fork parking area. Wildfires in the Red River Gorge Area have prompted forest rangers to close off a popular hiking section. A Daniel Boone National Forest supervisor issued an emergency closure order for the Auxier Ridge area October 24. He said the area was closed for safety reasons, since the path of a wild fire can be unpredictable. The fire began just after midnight October 23, and burned more than 115 acres before rain slowed its progress.

Source: <http://www.kentucky.com/2010/10/29/1499861/red-river-gorge-fire-spreads-to.html>

59. *October 29, WXYZ 7 Detroit* – (Michigan) **A fire is burning inside a state park.** Several fire departments in Michigan responded to a forest fire inside the Algonac State Park, and in the park land behind a residential neighborhood in Clay Township. Algonac City, Clay Township, Ira Township, Harsen Island, Marine City, and St. Clair fire stations all raced to the scene. The blaze was about 1 mile into the woods so firefighters had to walk or use all terrain vehicles to get to it. They were able to drive one tanker filled with water into the forest. The cause of the fire is unknown, but the fire scorched about a 1 mile path of leaves and brush. No one was injured but several firefighters were suffering from exhaustion. After about 2 hours, the fire was under control, and firefighters were just checking for hot spots.

Source: [http://www.wxyz.com/dpp/news/local\\_news/a-fire-is-burning-inside-a-state-park](http://www.wxyz.com/dpp/news/local_news/a-fire-is-burning-inside-a-state-park)

60. *October 29, KTRK 13 Houston* – (Texas) **Dry conditions led to grass fire in Trinity County.** At least 200 to 300 acres of pasture went up in smoke October 28 in Trinity County, Texas, after winds whipped fire through the dry grass. The fire threatened 25 to 30 homes, and because it has been so dry and windy, it was enough to make firefighters and residents nervous. Many of the residents in those homes outside of Trinity, north of Harris County, chose to evacuate the area because of the threat of the fire that was burning primarily pine land. Fire departments from all over that area, including firefighters from Trinity and Love Lady, along with the Texas Forest Service, worked to put the fire out. Firefighters got the fire under control overnight, but not before it burned a resident's hay barn and his pasture, which was home to about 80 head of cattle. The fire is under investigation.

Source: <http://abclocal.go.com/ktrk/story?section=news/local&id=7753067>

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

## **Dams Sector**

61. *October 29, Shreveport Times* – (Louisiana) **Corps looks at boosting Bodcau Dam safety rating.** For years, officials in Bossier Parish, Louisiana, have discussed the possibility of placing a control structure on the Bayou Bodcau Dam, which feeds water to other areas of the parish. The structure would enable streams to drain during floods by cutting off the flow, said the operations coordinator for the Bossier Levee District. However, to make this happen, the parish cannot simply purchase the structure and install it on the dam. A study must first be conducted to establish if the dam is safe enough to handle it. Bayou Bodcau Dam received a rating of 3 out of 5 (5 being the safest) from the Corps, which meant the dam was safe, but additional risk could not be added, a U.S. Army Corps of Engineers chief project manager said. "In a nutshell, if we hold back more water, we're increasing risk," he said. So, as part of a \$2 million study that began in 2007, the corps has started a geo-tech analysis to determine how to fix issues pertaining to the dam's rating. If fixed, the rating could increase, enabling a

structure to be safely put in place. The Corps funded half of the study, while the levee district, city and parish split the remaining cost. “Right now, we don’t know what upgrades would be needed to get the dam to a level four, but we should know within the next eight to 12 months,” he said.

Source: <http://www.shreveporttimes.com/article/20101029/NEWS01/10290322/Corps-looks-at-boosting-Bodcau-Dam-safety-rating>

62. *October 28, Associated Press* – (Wisconsin) **Watch lifted for western Wis. hydro dam.** Xcel Energy has lifted a watch for a western Wisconsin dam where a small sinkhole developed in an earthen embankment. An Xcel spokeswoman said the watch on the Big Falls hydroelectric dam near Ladysmith was lifted at 5:15 p.m. October 28. She said the sinkhole has stabilized. The utility had implemented a watch condition for potential failure of the dam October 26 as rain fell in western Wisconsin. As a precaution, Xcel began lowering the reservoir to relieve pressure. By the evening of October 28, the reservoir was down 9 feet; Xcel plans to eventually bring the water level down 12 feet. There were no evacuations. The dam is located on the Flambeau River about 7 miles north and east of Ladysmith.

Source: <http://www.wbay.com/Global/story.asp?S=13407837>

63. *October 28, WRCB 3 Chattanooga* – (Tennessee) **Surveillance shows twister slamming Chickamauga Dam.** The Army Corps of Engineers have released video of the tornado October 26 that struck the Chickamauga Dam in Tennessee. In the videos, the tornado can be seen touching down near the dam and then moving off toward the Lakeshore Apartments. In another of the videos, the several trailers at a construction site on the dam are seen being picked up and tossed into the river.

Source: <http://www.wrcbtv.com/Global/story.asp?S=13406411>

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

## **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 703-872-2267

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](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.