Top Stories

- According to a New York Times analysis of federal data, more than 20 percent of the nation’s water treatment systems have violated key provisions of the Safe Drinking Water Act over the last five years. The majority of violations have occurred at water systems serving fewer than 20,000 residents, where resources and managerial expertise are often in short supply. (See item 27)
- According to the Associated Press, authorities said a 20-year-old student is in custody after pointing a rifle at a teacher and firing shots in a classroom Tuesday at Northern Virginia Community College in Woodbridge, Virginia. (See item 32)

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. December 9, Nashua Telegraph – (New Hampshire) Investigation slams utilities over ice storm. Electric utilities in New Hampshire were ill prepared for the historic December 2008 ice storm that put 400,000 customers in the dark, 35,000 of them for more than a week, a state investigation concluded. “Utilities underestimated the
severity of this storm,” said the Public Utilities Commission (PUC) chairman. The Homeland Security and Emergency Management director said the state’s worst ice storm in known history has prompted power companies and state government to become better prepared for weather-related events like the snowstorm forecasted for Wednesday. The report concluded downed trees and limbs from the ice caused 85 percent of the outages. Utilities followed their own tree-cutting practices, but the most extensive damage came from trees and limbs outside utility cutting zones, the report said. It caused $80 million in damages to utility networks and another $70 million in damages to private businesses, residences, and nonprofit groups. A PUC consultant recommends Public Service Co. of New Hampshire (PSNH) get a Web-based, outage management system so it can inform the state and consumers the status of outages and updates on when power could be restored. PSNH is by far the state’s largest utility and the report notes it is the only one among the four electric power companies with neither a state-of-the-art outage management system nor plans to obtain one. Source: http://www.nashuatelegraph.com/news/statenewengland/472320-227/investigation-slams-utilities-over-ice-storm.html

2. **December 9, Associated Press** – (Texas) **Nobody hurt in fire at refinery.** A fire and explosion at the Motiva Enterprises LLC refinery complex in Port Arthur shut the hydrogen unit but caused no injuries. The accident occurred about 10:30 a.m. on December 8 in the hydrogen plant operated by Praxair Inc. A Praxair spokeswoman said all emergency systems operated as designed and “the situation was very quickly contained.” She told the Associated Press that about 10 Praxair employees were present when the accident occurred and nobody was hurt. The cause of the accident is being investigated. She had no details on what burned or a damage estimate, saying Praxair was assessing the situation. She said there was no damage to Motiva facilities or to the surrounding community. She said the Motiva refinery uses hydrogen in the production of low-sulfur gasoline. Source: http://www.amarillo.com/stories/120909/new_news19.shtml

3. **December 8, Arizona Republic** – (Arizona) **Crews busy restoring power in parts of the Valley after storm.** Arizona Public Service Company (APS) crews are busy attempting to restore power after a December 7 evening storm slammed the greater Phoenix area. As of 8:50 a.m., an APS spokeswoman said about 18,000 customers were still without power. At least 30 intersections across Phoenix are without traffic signals. The signal outages stretch from Central Avenue and Buckeye Road to 35th Avenue and Union Hills. At the high point of the storm, about 250,000 were without power stretching from Wickenburg to Scottsdale. The principal areas that power crews are dealing with are central and north-central Phoenix after trees were blown down over power lines. APS said it hopes to get everyone back online by noon, however, it could be later in the day before everyone is fully restored. APS said they are attempting to get extra resources on the scene, however road closures are making it a difficult task.
For another story, see item 46

Chemical Industry Sector

4. December 8, New Orleans Times-Picayune – (Louisiana) Fire department responds to chemical spill in Elmwood. Authorities say two people fell ill after a 300-gallon tank of hydrochloric acid spilled at Industrial Chemicals in Elmwood, Louisiana Tuesday afternoon. The incident occurred just before 4 p.m., according to a spokesman for the East Bank Consolidate Fire Department. The victims, women from a neighboring office building, suffered sore throats and nausea. But they declined treatment by paramedics, he said. The company almost immediately contained the spill. “The company is handling the clean-up procedure. The fire department is satisfied by the steps that were taken and we turned (the scene) back over to the company,” said the fire chief at the scene.

5. December 8, U.S. Environmental Protection Agency – (National) EPA issues 2008 information on toxic chemical releases. The U.S. Environmental Protection Agency released on December 8 the 2008 Toxics Release Inventory (TRI) which provides information on toxic chemicals used and released by utilities, refineries, chemical manufacturers, paper companies, and many other facilities across the nation. The TRI is compiled from data submitted to EPA and the States by industry. In EPA’s mid-Atlantic region, the 2008 TRI data indicate a 9.1 percent decrease of 35.2 million pounds of on and off site chemical releases as compared with 2007. A total of 350 million pounds of chemicals were released during 2008 to the air, water or landfills by facilities in the mid-Atlantic region which includes Pennsylvania, Delaware, Maryland, Virginia, West Virginia and the District of Columbia. When compared with the 2000 TRI data of 478.0 million pounds released, the 2008 figures represent a 27.0 percent reduction (128.0 million pounds) in toxic pollutants released by facilities in the region. This was accomplished by process modifications, raw material substitution and pollution control equipment. The lead and lead compound data for on and off site releases show an increase from 5.7 million pounds in 2007 to 6.6 million pounds in 2008. Since 2002 there has been a decrease of 1.6 million pounds from 8.2 million pounds to 6.6 million pounds in 2008. The mercury and mercury compound data show an increase from 45.3 thousand pounds in 2007 to 63.1 thousand pounds in 2008. In 2002 mercury and mercury compound releases were 61.6 thousand pounds.
Source: http://yosemite.epa.gov/opa/admpress.nsf/0/7BD33F484F46F5B885257686006AB25B

For more stories, see items 2 and 24
6. **December 9, Brattleboro Reformer** – (National) **Report: Spent fuel storage costs may run $225B.** If no federal repository for spent nuclear fuel is opened in the next 100 years, the nation’s taxpayers could be on the hook to pay for on-site storage, such as the dry casks at Vermont Yankee nuclear power plant in Vernon. That cost could run anywhere between $10 billion and $26 billion. That was the conclusion of the Government Accounting Office, which just released a report on the costs of nuclear waste management — whether it be a long-term repository, centralized storage or on-site storage. The United States has 70,000 tons of waste stored at 80 sites in 35 states. By 2055, the amount of waste is expected to increase to 153,000 tons. The GAO also conducted a scenario in which fuel stays on site for 500 years. It concluded the cost for that scenario could range between $34 billion to $225 billion. Because of the way the Nuclear Waste Policy Act was written, a fund established for the permanent disposal of spent fuel cannot be used for on-site or centralized storage. NWPA prohibits the Department of Energy from spending any money out of the fund for anything but Yucca Mountain in Nevada. The future of Yucca Mountain, which was identified as the long-term location for the storage of nuclear waste, is uncertain. The Presidential administration recently announced it would not support further work to develop the site, essentially saying no spent fuel will ever be stored there. Source: [http://www.reformer.com/localnews/ci_13956508](http://www.reformer.com/localnews/ci_13956508)

7. **December 8, U.S. Nuclear Regulatory Commission** – (National) **NRC chairman Gregory B. Jaczko remarks at today’s meeting about public comments on proposed emergency preparedness rule changes.** The Commission met Tuesday to hear comments and discuss the proposed changes to the emergency preparedness requirements for licensees. Tuesday’s meeting reflected the Commission’s critical focus on ensuring the safety and security of the nation’s licensed facilities and the American public. The proposed regulations seek to ensure adequate and timely emergency response through several measures. These include provisions to prevent onsite emergency responders from being stretched too thin by the assignment of additional responsibilities, efforts to enhance the coordination between onsite personnel and local and state emergency responders, and other measures intended to strengthen the ability of licensees to effectively implement their emergency plans. Source: [http://www.nrc.gov/reading-rm/doc-collections/news/2009/09-195.html](http://www.nrc.gov/reading-rm/doc-collections/news/2009/09-195.html)

For another story, see item 31

[Return to top]

**Critical Manufacturing Sector**

8. **December 8, U.S. Consumer Product Safety Commission** – (National) **Goodman Company reannounces recall of air conditioner/heat pump units due to fire hazard.** The U.S. Consumer Product Safety Commission, in cooperation with Goodman Company, LP, on December 8 announced a voluntary recall of about 30,000
Packaged Terminal Air Conditioner/Heat Pump (PTACs) Units, which were previously recalled in August 2008. The power cords on the PTACs can overheat, posing a burn or fire hazard. Goodman has received eleven reports of smoke or fire associated with the PTAC’s power cords. No injuries have been reported. The recall includes 5.0 kW Amana-brand, Comfort-Aire-brand, and Century-brand Packaged Terminal Air Conditioner units with model numbers PTxxx3x50xx (Amana) and EKTxxx-150x (Comfort-Aire and Century) and serial numbers 0702112056 through 0804237539. The model and serial numbers are located on the control board plate found under the PTAC unit’s front cover. Goodman and heating and cooling equipment dealers nationwide from February 2007 through June 2008 for between $700 and $1,000. Consumers should contact Goodman to receive a free replacement power cord. Commercial and institutional owners will be contacted directly and will install the power cord.

Source: http://www.cpsc.gov/cpscpub/prerel/prhtml10/10058.html

9. December 8, Associated Press – (Illinois) Federal board to investigate deadly Ill. explosion. The U.S. Chemical Safety Board says it is sending a team to northern Illinois to investigate a gas line explosion at a technology plant that left one man dead. A board spokeswoman said on December 8 that the team should arrive in Belvidere on December 9 at the plant of NDK America Inc. On December 7, the explosion sent debris aloft that killed an Indiana truck driver at a nearby highway rest area. The plant employs about 30 people and makes synthetic crystals for computers. According to a news release from the board, it does not issue citations or fines but does make safety recommendations.

Source: http://www.wifr.com/home/headlines/78784447.html

10. December 5, Los Angeles Times – (National) Toyota vehicles in another federal safety probe. Federal safety officials have opened a probe into two models of Toyota Motor Corp. vehicles after drivers complained that their cars inexplicably stalled in traffic, sometimes at highway speeds. The National Highway Traffic Safety Administration (NHTSA) posted a document the week of November 30 launching the investigation into Toyota’s Matrix and Corolla cars. It is the latest in a string of quality-related issues for the Japanese automaker in recent months. The document cited 26 complaints from drivers of 2006 model year Matrix and Corolla vehicles. Consumers “allege stalls occurring randomly while driving, including some on highways and some in intersections,” the agency said. In addition to the Corolla and Matrix probe, which covers 397,000 vehicles, NHTSA is investigating the 2003 Sequoia, based on allegations that the electronic stability control system seizes control of the brakes at inappropriate times. One such event details a Corolla that stalled in heavy traffic in December of last year, blocking a right-turn lane for two hours until it could be towed. The agency indicates that the problem could be linked to the electronic control module, or onboard computer.

11. December 9, Alamogordo Daily News – (New Mexico) **Wind blows off roof at WSMR.** High winds on December 8 blew the roof off of a building at White Sands Missile Range (WSMR). A spokeswoman for White Sands Public Affairs said the winds blew the roof off of the Directorate of Plans, Training, Mobilization and Security building at about 6:30 a.m. Tuesday. “It’s a pretty large building,” she said. She said the building has two stories and is about 30,000 square feet in area. She said everyone inside was safely evacuated. The spokeswoman said at one point, winds were clocked at about 95 mph blowing through San Agustine Pass. She said much of the base lost power during the stormy conditions. She said the installation was still open on December 8, but nonessential personnel working in areas that did not yet have power restored were sent home. “Other than that, we’re still functioning business as normal,” she said. According to a news release issued by WSMR, two people from the building were treated for injuries at the base’s McAfee Army Health Clinic and released. The building acts as the post’s police station, but the release states police services remained operational from an alternate location. The release states winds also downed power lines, uprooted trees and caused minor damage to other buildings and vehicles. Source: [http://www.alamogordonews.com/ci_13956748](http://www.alamogordonews.com/ci_13956748)

12. December 8, San Francisco Examiner – (California) **Marine fueling station to receive needed repairs.** Major repairs are planned next year for an aging marine fuel station near Aquatic Park that is used to fill the tanks of Coast Guard cutters, tugs, bar pilot boats, and other small vessels. Load and berthing restrictions currently apply to the Hyde Street Harbor Fuel Dock, which is a Port of San Francisco-owned facility that’s operated by General Petroleum, because its substructure has become dilapidated. The Port will soon begin seeking bids from contractors interested in repairing the facility by installing steel frames to support the structure and adding composite fenders around the pier’s perimeter. At least one vessel will be able to fuel at a time while the repairs are under way, Port documents show. Repairs are expected to begin in May and finish by next December. Source: [http://www.sfexaminer.com/opinion/blogs/under-the-dome/Marine-fueling-station-to-receive-needed-repairs-78795332.html](http://www.sfexaminer.com/opinion/blogs/under-the-dome/Marine-fueling-station-to-receive-needed-repairs-78795332.html)

13. December 6, Agence France-Presse – (International) **After long delay, Airbus A400M to fly for 1st time.** The Airbus A400M military plane is scheduled to take to the skies on its first test flight the week of December 7 after a long delay that has caused headaches for European defense group EADS and the loss of a client. The A400M was to replace aging military cargo carriers in several European air forces but its development has been dogged by a series of serious technical problems. Some governments have begun to tire of waiting for Airbus to resolve the issues, and French and German officials have given the firm until the end of the year to prove that the project remains viable. The delays have cost millions and forced Airbus to renegotiate its contracts with several customers. South Africa has dropped its order entirely and Britain has mulled switching its business to U.S. manufacturers. Source: [http://www.defensenews.com/story.php?i=4407177&c=EUR&s=AIR](http://www.defensenews.com/story.php?i=4407177&c=EUR&s=AIR)
For another story, see item 9

Banking and Finance Sector

14. December 9, The Register – (International) **Scammers scrape RAM for bank card data.** In the wake of industry rules requiring credit card data to be encrypted, malware that siphons clear-text information from computer memory is all the rage among scammers, security researchers say. So-called RAM scrapers scour the random access memory of POS, or point-of-sale, terminals, where PINs and other credit card data must be stored in the clear so it can be processed. When valuable information passes through, it is uploaded to servers controlled by credit card thieves. While RAM scrapers have been around for a few years, they are a “fairly new” threat, according to a report released Wednesday that outlines the 15 most common attacks encountered by security experts at Verizon Business. They come in the wake of Payment Card Industry rules that require credit card data to be encrypted as it passes from merchants to the processing houses. “They are definitely a response to some of the external trends that have been going on in the cybercrime environment,” says a research and intelligence principal for Verizon Business. “Within a year, we’ve seen quite a few of them in the wild.” Verizon employees recently found the malware on the POS server of an unnamed resort and casino that had an unusually high number of customers who had suffered credit card fraud. The malware was sophisticated enough to log only payment card data rather than dumping the entire contents of memory. That was crucial to ensuring the malware did not create server slowdowns that would tip off administrators. The RAM scraper dumped the data onto the server’s hard drive. The perpetrators visited at regular intervals through a backdoor on the machine to collect the data. Source: [http://www.theregister.co.uk/2009/12/09/ram_scraper_credit_card_theft/](http://www.theregister.co.uk/2009/12/09/ram_scraper_credit_card_theft/)

15. December 9, Napa Valley Register – (California) **Ponzi scheme flowed through Napa bank, lawsuit alleges.** Nearly $200 million in a suspected Ponzi scheme flowed through Napa’s branches of Washington Mutual Inc., according to a class-action suit filed recently in San Francisco. The suit filed on behalf of 1,000 investors in the U.S. District Court for the Northern District of California alleges that WaMu facilitated fraud by depositing checks for Millennium Bank, a Caribbean bank that sold bogus high-yield certificate of deposits over the Internet to American and Canadian investors. JPMorgan Chase is named in the suit because it assumed WaMu’s liabilities when it bought the troubled bank in September 2008. A report the SEC Receiver filed last week in federal court estimates the fraud totaled $246 million between 1996 and 2009 — $178 million more than federal regulators had estimated when they filed their complaint in March. But forensic accountants continue to analyze the data, said a Dallas attorney who worked on the report. According to federal regulators, investors believed they were putting their money in a financial institution with ties to a Swiss bank. Instead, federal investigators suspect, investors sent checks or wire transfers to the bank in the Caribbean island of St. Vincent, where the funds were bundled and sent by FedEx to Napa. In Napa, two defendants are suspected of depositing the funds under
various accounts at WaMu banks.
Source:

16. December 9, Deutsche Presse-Agentur – (International) Report: French tax-fraud investigators have stolen Swiss bank data. An employee for the Swiss bank HSBC in Geneva stole data from thousands of secret bank accounts and handed the information to French tax-fraud investigators, the daily Le Parisien reported on December 9. This alleged data theft may have been the source for the list of 3,000 owners of secret Swiss bank accounts that the French Budget Minister said in August were being investigated for tax fraud. The former HSBC employee was a manager in the bank’s computer services department and currently lives in France under a false identity. The accounts cracked by the former HSBC employee reportedly include those of a well-known French comedian and several politicians, a source close to the investigation told Le Parisien. Some accounts were listed under codes that suggested they belonged to intelligence services. Other accounts belonged to Colombian nationals and ‘Chinese authorities,’ the source said. In a first reaction, HSBC confirmed that data had been stolen, but said it involved ‘not more than 10 clients’ and that the ‘data are old and not sensitive.’
Source:

Transportation Sector

17. December 9, Federal Bureau of Investigation – (Florida) Florida man arrested for assaulting a flight attendant. A United States Attorney announced a criminal complaint against a Florida man for interfering with a flight crew attendant. If convicted of the charges, the man faces a maximum penalty of 20 years in federal prison. According to the complaint, on November 30, 2009, the man interfered with a flight attendant’s ability to carry out her duties while he was a passenger aboard Continental Airlines Flight 3132 from Houston, Texas to Jacksonville, Florida. He allegedly charged toward the flight attendant in the direction of the cockpit of the plane and then was subdued by other passengers, including an FBI agent traveling on the flight. Federal law makes it a crime to intimidate and assault flight crew and flight attendants on an aircraft within the special aircraft jurisdiction of the United States when such actions interfere with the flight crew’s performance of its duties.
Source: http://www.webnewswire.com/node/487726

18. December 9, Deutsche Presse-Agentur – (International) Ukraine police destroy suspected bomb on Russian train. Police destroyed a suspected bomb found aboard a Russian train while it was passing through Ukraine’s Kharkiv province, the Interfax news agency reported Wednesday. A conductor aboard a passenger express running
between the Russian city of St. Petersburg and the Ukrainian city of Sevastopol discovered the device Tuesday evening as the train was passing through Kharkiv province, in eastern Ukraine. Ukrainian railroad managers routed the train onto an isolated sidetrack, evacuated passengers and notified law enforcement officials. A police bomb squad removed the package from the train and destroyed it nearby in a controlled explosion. No injuries were reported, and the train continued its southward journey before midnight, said a spokesman for Ukraine’s Emergency Situations Ministry. The discovery of a suspected explosive device came less than two weeks after a high-speed express train traveling between Moscow and St Petersburg was bombed, killing a total 27 passengers and railroad staff. Russian law enforcement officials have blamed terrorists, possibly ethnic Chechen or Ingush insurgents for the attack.


19. December 8, Cordele Dispatch – (Georgia) Arrests made in railroad theft attempts. Responding to tips that railroad tracks were being taken from two locations, Crisp County Sheriff’s Department deputies arrested two men in connection with those incidents on December 1. One man found at the scene told the officer he was working for another man who had left the area to acquire a chain. When the second man returned, he told the officer he had been given permission by a railroad marshal whose name he could not remember to take the rails. That statement could not be verified. About 40 feet of rail valued at $175 a foot had been damaged and could not be reused. In responding to a second complaint from Crossroad Store Rd., a policewoman said she saw a wrecker loaded with railroad connectors. The vehicle driver told the officer he, too, had been given permission to take the items. A railroad employee called to the scene said no one had permission to remove anything and that the items loaded the truck were valued at $1,500. The truck’s driver was subsequently charged with criminal attempt to commit theft and criminal trespass.


20. December 8, Boston Herald – (National) Feds ask for power to oversee rail transit safety. The Presidential Administration asked Congress December 8 to give the federal government power to oversee the safety of subways, light rail, and other urban train systems. The Transportation Secretary, in testimony before a House panel, outlined a plan to give the Federal Transit Administration authority to set standards for and inspect the nation’s 50 local rail transit systems in 27 states. Currently there are no nationwide minimum standards for rail transit safety, only voluntary standards produced by industry groups. The administration sent a legislative proposal to House and Senate leaders that would effectively eliminate a legal prohibition in place since 1965 that prevents the federal government from imposing broad transit safety standards. The Transportation Secretary also announced the formation of an advisory committee to help develop new safety regulations. “The current system for federal rail transit safety oversight is weak and inadequate and does not guarantee a consistent level of safety for transit passengers,” the Secretary said. The head of the transit administration told the House Transportation and Infrastructure Committee that with
the exception of California, which he called the “gold standard,” states have an average of less than one safety inspector per rail transit system. Some lawmakers noted that rail transit systems overall have a significantly lower accident rate than freight or long-distance passenger trains, which are subject to federal safety regulation. They questioned whether imposing new regulations would be burdensome on systems that for the most part are already very safe.


For more stories, see items 46 and 50

[Return to top]

Postal and Shipping Sector

21. December 8, Oakland Tribune – (California) Three envelopes, three causes for concern in Alameda County. Three separate envelopes, each containing a suspicious white powder, arrived at two East Bay police departments and a courthouse Tuesday. No one was injured. An Alameda County sheriff said an envelope containing an unknown white powder arrived in the day’s mail Tuesday afternoon at the Sheriff’s Office at 14th and Oak streets near downtown Oakland. The floor where the envelope was delivered was quarantined while sheriff’s deputies investigated. It was not known late Tuesday what the powder was. The delivery in Oakland came after an evacuation at 12:30 p.m. Tuesday at the Hayward police station. A mailroom employee opened a letter containing a white powder that later was determined to be a nonhazardous substance. Two people were exposed to the powder and quarantined until the all-clear was given around 2:30 p.m., said a Hayward police spokeswoman. The letter was addressed to the Hayward Police Department. A similar letter containing powder was found at the nearby Hayward Hall of Justice, but that facility was not evacuated, police said.


[Return to top]

Agriculture and Food Sector

22. December 8, Reuters – (International) Russia bans pork from five U.S. plants - USDA. Russia gave no reason for the bans of pork in the USDA report. The five plants include three owned by Smithfield Foods Inc, and one by Tyson Foods Inc. The fifth is Sioux-Preme Packing Co in Sioux Center, Iowa. The Smithfield plants are in Sioux Falls, South Dakota; Sioux City, Iowa; and Tar Heel, North Carolina, the latter being the largest pork plant in the world. The Tyson plant is in Madison, Nebraska.

Source: http://www.reuters.com/article/idUSN0821881220091208?type=marketsNews
23. **December 8, USAgNet – (Virginia) H1N1 flu hits Virginia turkey flock.** The USDA Animal Plant Health Inspection Service (APHIS) has reported a new outbreak of influenza A H1N1 in a turkey flock in the state of Virginia. APHIS sent an Immediate Notification dated November 30 to the World Organization for Animal Health. The outbreak started on November 16 in an unspecified location in Virginia in a flock of 3,270 turkey breeder hens in a commercial flock. No other barns on the farm are reported to be affected and no other birds have shown signs of clinical illness. APHIS and the Virginia Department of Agriculture and Consumer Services are conducting a comprehensive epidemiological investigation of this event. According to the report, a significant drop in egg production was observed in one barn only in the week of November 16. A week later, presumptive detection of 2009 pandemic A/H1N1 was reported to APHIS and laboratory samples were submitted to the National Veterinary Services Laboratories (NVSL). NVSL confirmation of 2009 pandemic A/H1N1 influenza virus on November 30. Information points to recent exposure of the turkeys to a farm worker exhibiting influenza-like symptoms. The farm was and continues to be under enhanced biosecurity.


24. **December 8, Worthington Daily Globe – (Minnesota) JBS investigates small ammonia leak.** The Worthington Fire Department, Worthington Rescue, three Worthington Ambulances, and the local police department responded to a small ammonia leak 8:30 a.m. Tuesday at JBS meat packing plant. According to a JBS spokesperson, some contractors were working on the plant’s roof-top refrigeration unit when ammonia leaked out and a small amount was sucked into the ventilation system. Five people working in the area were evacuated and transported to Sanford Regional Hospital Worthington, where they were observed and later released. All were told they could have the remainder of the day off, but three of them returned to work at the plant, the spokesperson said. He said the ammonia leak was reported by the workers on the roof, and that workers inside the plant had not reported any issues. JBS is conducting an investigation regarding what exactly happened and how it happened to prevent future ammonia leaks.


---

**Water Sector**

25. **December 8, San Diego Union-Tribune – (California) Water main break in Mountain View causes flooding.** A 30-inch cast-iron water main ruptured in the Mountain View neighborhood in San Diego Tuesday afternoon, sending thousands of gallons of water into surrounding streets and yards and flooding at least one home, authorities said. The break was reported about 3:30 p.m. near the intersection of South 35th and Durant streets, said a spokesman for the city of San Diego Water Department. Water was shut off by 6:40 p.m. Twenty customers were without water, and some other residents in the area have lower water pressure, he said. The spokesman said that a temporary line to provide water for residents should be installed by 6 a.m. Wednesday.
The main was not expected to be repaired until late Wednesday afternoon. Crews originally believed the rupture occurred in an 8-inch pipe that runs parallel to the 30-inch pipe. They quickly shut off water in the smaller pipe, but the water kept coming. A special crew trained in hydraulics was called in to shut off the water in the large-diameter pipe. The rupture also caused a large sinkhole to form at the intersection of South 35th and Durant streets. Streets are closed at least one block in every direction from the location of the break.

26. December 8, WALB 10 Albany – (Georgia) **Water tower accident under investigation.** OSHA is investigating what led to a water tank accident Monday in Homerville, Georgia. Two workers cleaning a tank were injured when the two and a third man fell into the tank. The two workers who were injured from Monday night’s fall from a Homerville water tower are still in the hospital. The cause of the fall has still not been determined. A third man walked away with no injuries. OSHA plans to interview the crew leader to find out exactly what happened. Utility workers were rescued after falling down this tower. They were sand blasting inside the 500,000 gallon tank which is a common practice before panting the tank. Emergency workers at the scene last night say this was the first time they have ever heard of this kind of water tank emergency. They called for help from the Lowndes and Valdosta firefighters who are a part of the Georgia Search Rescue Team trained for this type of rescue. The men’s fall was broke by a safety net but they had to be lowered down the middle the rest of the way. The City of Homerville has been using Utility Services company for routine maintenance of their tanks.

27. December 7, New York Times – (National) **Millions in U.S. drink dirty water, records show.** More than 20 percent of the nation’s water treatment systems have violated key provisions of the Safe Drinking Water Act over the last five years, according to a New York Times analysis of federal data. That law requires communities to deliver safe tap water to local residents. But since 2004, the water provided to more than 49 million people has contained illegal concentrations of chemicals like arsenic or radioactive substances like uranium, as well as dangerous bacteria often found in sewage. Regulators were informed of each of those violations as they occurred. But regulatory records show that fewer than 6 percent of the water systems that broke the law were ever fined or punished by state or federal officials, including those at the Environmental Protection Agency (EPA). Studies indicate that drinking water contaminants are linked to millions of instances of illness within the United States each year. In some instances, drinking water violations were one-time events, and probably posed little risk. But for hundreds of other systems, illegal contamination persisted for years, records show. An analysis of EPA data shows that Safe Drinking Water Act violations have occurred in parts of every state. The problem, say current and former government officials, is that enforcing the Safe Drinking Water Act has not been a federal priority. The majority of drinking water violations since 2004 have occurred at water systems serving fewer than 20,000 residents, where
resources and managerial expertise are often in short supply. It is unclear precisely how many American illnesses are linked to contaminated drinking water. Scientific research indicates that as many as 19 million Americans may become ill each year due to just the parasites, viruses and bacteria in drinking water.  

For another story, see item 46

Public Health and Healthcare Sector

28. **December 9, Forbes** – (Associated Press) **Patient accused of shooting doctor at Ky. clinic.** A patient who made threats after being denied narcotics at a rural Kentucky clinic returned and shot his doctor to death, police said. A Perry County sheriff’s deputy said the man had asked for narcotics but was required to give a urine sample, which he refused to do. “From that point, he got real angry, he just went crazy, and he made a threat he was going to come back and blow up the building,” said the police officer who responded when the clinic in Cornettsville called about the threat. Clinic officials did not want to press charges, so the deputy left. The man returned later and shot the doctor. After the shooting, state police took over the investigation.  

29. **December 9, Bloomberg** – (International) **Roche’s Tamiflu not proven to cut flu complications, study says.** Roche Holding AG’s antiviral drug Tamiflu may not prevent complications from influenza in healthy adults, according to a review by an independent research group that reversed its previous findings that the medicine warded off pneumonia and other deadly conditions linked to the disease. The pill has been the mainstay of treatment for pandemic swine flu, which has killed nearly 9,000 people since it emerged in April, according to the World Health Organization. Roche, based in Basel, Switzerland, defended the benefits of the drug, which it expects to generate $2.64 billion in sales this year. An analysis of 20 studies by the Cochrane Collaboration showed Tamiflu offered mild benefits for healthy adults and found no clear evidence it prevented lower respiratory tract infections or complications of influenza, according to the group. The review, published in the British Medical Journal and broadcast yesterday on the U.K.’s Channel 4 News, showed the drug eased and shortened symptoms if taken quickly.  

30. **December 8, KTVU 2 San Francisco** – (California) **Walnut Creek gas leak forces Kaiser Medical offices evacuation.** A construction crew ruptured a gas line in Walnut Creek, California, Tuesday, prompting the evacuation of two Kaiser Permanente buildings and a PG&E building, a utility spokeswoman said. “There was a concern that there might be some gas in the building, so they shut off the power to the building,”
Contra Costa’s County Fire Protection District spokeswoman said. One of the Kaiser buildings that was evacuated contained pediatric and women’s health offices; the other contained eye care and physical therapy offices, a PG&E spokeswoman said. A Kaiser Permanente spokesman said all of the buildings are outpatient facilities.


31. December 8, WAFF 48 Decatur – (Alabama) Radiation overdose claim has FDA investigating Huntsville Hospital. Hair loss and redness of the skin are just two of the symptoms a local woman claims she suffered after undergoing a medical procedure at Huntsville Hospital. Her claims have even caught the attention of the U.S. Food and Drug Administration. In September, the woman said she went into Huntsville Hospital for a CT brain scan, but said something went wrong. Now she is part of a full scale investigation from the FDA. The woman’s attorney said the excess radiation could have been caused by human error or the machine malfunctioning, but the woman received 12 to 14 times the amount of radiation required. He said a malpractice law suit against the hospital and the manufacturer of the machine may be the next plan of action. “There is no backup, there is no safety check, there is no dual-system and certainly the manufacturers will have to address that to provide for a greater safety,” he added.


For another story, see item 37

32. December 9, Associated Press – (Virginia) Student fires shots in Va. college. Authorities said a 20-year-old student is in custody after pointing a rifle at a teacher and firing shots in a classroom at a community college in Virginia. No injuries are reported. The shooting happened Tuesday afternoon at Northern Virginia Community College’s campus in Woodbridge, about 25 miles south of Washington, D.C. The suspect, of Manassas, is charged with attempted murder and discharging a firearm in a school zone. He is being held without bail. Prince William County Police spokeswoman said the “upset student” was armed with a high-powered rifle. The teacher dropped to the floor when she saw the gun. Officials say the gunman fired two shots then stopped without explanation and left the classroom. He was arrested in the hallway. He did not have the gun when he was arrested, but told police where it was, a Prince William County Police spokeswoman said. The college enacted its emergency lockdown procedures and later issued a statement saying all Woodbridge classes were canceled Tuesday because of the shooting.


33. December 9, Ledger-Enquirer – (Georgia) Army offers reward in Fort Hood-type threat on Fort Benning. The United State Army Criminal Investigation Command is offering a $5,000 reward for information leading to the apprehension and conviction of
the person or persons responsible for leaving a suspicious package with a threatening note last month on Fort Benning. The package was found November 19 by military police in a gazebo adjacent to Building 9111 on Kelley Hill. A post public affairs spokeswoman said officers were alerted to the situation by a 911 caller. The Army Times reported the package contained 20 hollow-point bullets and an anonymous note threatening an attack similar to the one at Fort Hood. A press release emailed Tuesday from the CID confirmed a “small amount of ammunition” was contained within the box.


34. **December 9, Orlando Sentinel** – (Florida) **Three students arrested in acid-bomb explosion at Cypress Creek High School.** Three Cypress Creek High School students were arrested and accused of making an acid bomb that exploded at the school and injured a school worker, according to the Orange County Sheriff’s Office. The students are charged with “placing and making a destructive device,” according to a news release. The Orlando Sentinel is not naming the boys because they are juveniles. Two are 16. One is 14. Deputies responded to the school, 1101 Bear Crossing Drive, in east Orange County at 7:20 a.m. Tuesday after the device blew up. The school was placed on lockdown following the incident. No students were injured. The homemade explosive was detonated in a courtyard near the school’s administrative offices, the sheriff’s office said. An employee burned his right index finger when he moved it out of the way after it detonated, reports show. The area was secured by the school resource officer after the explosion. The arrests were announced Wednesday morning.


35. **December 8, DarkReading** – (National) **Hacker exposes unfixed security flaws in Pentagon Web site.** A Romanian hacker has posted a proof-of-concept attack exploiting vulnerabilities on the Pentagon’s public Web site that were first exposed several months ago and remain unfixed. The hacker, who goes by Ne0h, demonstrated input validation errors in the site’s Web application that allow an attacker to wage a cross-site scripting (XSS) attack. The XSS vulnerability had been previously disclosed by at least two other researchers several months ago — and Ne0h’s findings show the bug is still on the site. The site, which is run by the Office of the Assistant Secretary of Defense for Public Affairs, is basically a tourist site for the Pentagon and does not appear to house any sensitive data. But a security researcher who studied the Ne0h’s work says the Pentagon Web site could be used to redirect users to a malicious site posing as the Pentagon site.

Source: [http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=222001155&subSection=Vulnerabilities+and+threats](http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=222001155&subSection=Vulnerabilities+and+threats)

36. **December 7, U.S. Government Accountability Office** – (International) **Diplomatic Security’s recent growth warrants strategic review.** In a report completed on November 12, 2009, but released on December 7, 2009, the GAO addressed the current state of the Diplomatic Security Service. Diplomatic Security’s mission, to ensure a
safe environment for the conduct of U.S. foreign policy, involves activities such as the protection of people, information, and property overseas, and dignitary protection and passport and visa fraud investigations domestically. These activities have grown since 1998 in reaction to a number of security incidents. Diplomatic Security funding and personnel have also increased considerably over the last 10 years. In 1998, Diplomatic Security’s budget was about $200 million; by fiscal year 2008, it had grown to approximately $1.8 billion, of which over $300 million was for security in Iraq. In addition, the size of Diplomatic Security’s direct-hire workforce has doubled since 1998 and will likely continue to expand. Recently, Diplomatic Security’s reliance on contractors has grown to fill critical needs in high-threat posts. Diplomatic Security faces several challenges that could affect the bureau’s ability to provide security and use its resources efficiently. First, State’s policy to maintain missions in increasingly dangerous posts requires a substantial amount of resources. Second, although Diplomatic Security’s workforce has grown considerably over the last 10 years, staffing shortages in domestic offices and other operational challenges—such as inadequate facilities, language deficiencies, experience gaps, and balancing security needs with State’s diplomatic mission—further tax its ability to implement all of its missions. Finally, Diplomatic Security’s tremendous growth has been in reaction to events and does not benefit from adequate strategic guidance. Neither State’s departmental strategic plan nor Diplomatic Security’s bureau strategic plan specifically addresses the bureau’s resource needs or management challenges.


For more stories, see items 37, 47, and 49

[Return to top]

Emergency Services Sector

37. December 7, Washington Times – (District of Columbia) Capitol Police papers found on street. Internal U.S. Capitol Police documents marked as “law enforcement sensitive” containing maps from near where a congressional leader lives to a relative’s house were found near a curb recently in front of a 7-Eleven convenience store in Washington. The 10 pages of U.S. Capitol Police dignitary protection unit papers also include information on the security systems in place at a hospital along the mapped route in Maryland. The documents were dated November 19. The papers were found near a curb on Maryland Avenue and Eighth Street in Northeast Washington by an employee of the Washington Times. The Capitol Police, which has a special unit that protects the leaders of Congress, said that the release of the information never compromised security and that the data, while marked sensitive, is publicly available. But the director of security for the Shore Health System in Easton, Maryland called the information release troubling and said he planned to call for an explanation from Capitol Police officials. The documents found on the roadside included information on the hospital’s internal systems that he said would not be released to the public. “One of my concerns about these documents from a law enforcement perspective is that they disclose and provide unnecessary insight into law enforcement methods and
procedures,” said the director of operations at SES Resources International Inc. and a retired special agent in charge for the U.S. Immigration and Customs Enforcement in New York.

38. December 7, U.S. Department of Justice – (National) U.S. settles lawsuit with Itochu Corp. and Itochu International regarding defective bullet-proof vests. The United States has reached a $6.75 million settlement with Itochu Corp. of Japan and its American subsidiary, Itochu International Inc., to resolve claims under the False Claims Act in connection with the companies’ importation and sale of defective Zylon fiber used as the key ballistic material in bullet-proof vests purchased by the United States for federal, state, local and tribal law enforcement agencies, the Justice Department announced. The Itochu companies imported the Zylon fiber on behalf of the Zylon manufacturer, Toyobo Co. Ltd. of Japan. The United States alleged that the Itochu companies were aware that the fiber degraded quickly over time and that the companies knew that this degradation rendered bullet-proof vests containing woven Zylon unfit for use. The government further alleged that, despite this knowledge, Itochu personnel actively participated in the marketing of the Zylon fiber and downplayed the extent of the degradation problem. “This agreement resolves our allegations that these defendants wasted taxpayers dollars by failing to address problematic vests even after they were aware of them.” This settlement is part of a larger government investigation of the industry’s use of Zylon in body armor. As part of the agreement, Itochu has pledged its cooperation in the government’s ongoing investigation.

For more stories, see items 11 and 21

Information Technology Sector

39. December 9, ITProPortal – (International) Botnets set to become smarter in 2010. If findings of a recent research study are to be believed then instead of putting an effective check on spamming activities, people are increasingly falling victim to fraudulent activities on the online space. An annual security research report from Symantec’s MessageLabs division has presented a grotesque picture of the cyber security landscape, with the report claiming that the spamming traffic accounted for a massive 87.7 percent of the total email traffic in 2009. The spamming activity was highest in the month of February with 90.4 percent of overall email traffic, while it reached its lowest in May when it was 73.3 percent. A significant rise has been noted in the volume of junk mails from the past year when the spam rate is around 81.2 percent. The most striking part of the report is that the majority of this spamming activity (around 83.4 percent) was attributed to zombie machines, indicating the extent to which the rogue applications are controlling the PCs across the globe. The closure of a couple of botnet hosting ISPs, including McColo in 2008 and Real Host in August, has
prompted cybercrooks to re-engineer their botnets to take the reins of the control and command system within hours, rather than weeks of relative calmness followed by the shutdown of McColo. Citing the same, a key analyst with the firm said in a statement: “The McColo outage had a huge impact on spam volumes as it took a few weeks for spammers to recover, but we’ve seen this year botnet technology has evolved so that there is no longer a single point of failure.”

40. December 8, Computer Weekly – (International) **Criminals outwit Captcha Web site security systems.** According to research by Symantec and MessageLabs, criminals have developed software capable of decoding the hidden text in Captcha pictures, which are meant to distinguish genuine customers from automated software. The groups are using the technology to create thousands of accounts on legitimate webmail sites and social networking sites, which they can use to launch spam and phishing attacks against web users, says a senior analyst at Symantec. “If you have a large number of legitimate accounts on a site, you can benefit from the legitimate domains. It becomes very difficult for anti-spam technology to identify messages from those domains as spam. It is hard to block, because you risk blocking legitimate users,” he says. The practice is putting businesses at risk, which can be on the receiving end of credible looking e-mails containing links to malware. “Social networking and microblogging sites are coming under a lot of pressure from the bad guys. They are creating legitimate profiles and even phishing for accounts of real people,” he says. “There are inherent risks for organizations that do not have controls in place.” In some cases, cybercriminals are using image recognition software to decode the disguised words in Captcha pictures. Others groups have developed software that is capable of decoding the audio version of Captcha intended for people who have difficulty reading Web sites, by analyzing the waveforms to recognize the letters of each code word. Specialist companies have also sprung up, which hire people to create accounts on Web applications, paying them $2 or $3 per thousand. They sell the accounts on to criminal groups for between $30 and $40 a thousand, said the analyst.

41. December 8, MSNBC – (International) **Surprise! Merchants say Web fraud is down.** Online merchants in the U.S. and Canada report a dramatic 18 percent drop in fraud, down from $4 billion in 2008 to $3.3 billion this year, according to a survey by the security firm CyberSource. Meanwhile, the fraud rate of 1.2 percent of all sales is the lowest in the 11-year history of the survey. Even among international orders, traditionally the bane of Web sites, fraud rates plummeted by 50 percent. The news comes just in time for Web shoppers who are pulling out their credit cards and wondering about the safety and security of online holiday gift shopping. “We were surprised,” said CyberSource’s director of market and customer intelligence. “Internally people were thinking that with the recession, fraud would go up, that there would be more people out there with technical skills who needed to put food on the table. But it looks like the merchants stepped up to the plate and got their act together.”
The director said the recession may actually have helped Web site fraud departments in two ways: prompting online firms to implement tighter fraud controls to chase down every dollar during the tough economy and giving computer security professionals at these Web sites a chance to catch their breath. But new technologies undoubtedly contributed to the fight against fraud. This year, a relatively new technique called device fingerprinting, which can make life very difficult for would-be credit card thieves, took hold in the marketplace. Device fingerprinting goes far beyond cookies and IP addresses to identify users, employing software to examine a variety of unique identifiers on computers used to order products. These range from the version of Flash software stored on a computer to the time and date stamp of the installed Web browser and the version of BIOS used inside the machine. Combining these characteristics, the software can positively identify computers with accident rates as low as one in 1 million, the director said.


42. *December 8, Washington Post* – (International) **Critical updates for Adobe Flash, Microsoft Windows.** Microsoft released six software updates on December 8 to fix at least a dozen security vulnerabilities in Windows, Internet Explorer, Windows Server and Microsoft Office. More than half of the flaws earned a “critical” rating, meaning criminals could exploit them to break into vulnerable systems without any help from users. Separately, Adobe Systems Inc. issued critical security updates to its Flash Player and AIR Web-browser plugins. The updates are available from the Windows Update Web site, or via the Automatic Update feature in Windows. Probably the most important update for most users is the one for Internet Explorer, which corrects five critical flaws in IE 6, 7 and 8. These are vulnerabilities that attackers could exploit to quietly install malicious software on a user’s machine if a user browses with IE to a hacked or booby-trapped site. Adobe also issued security updates to its ubiquitous Flash Player and its Adobe AIR software. Updates are available for Windows, Linux and Mac versions of these programs. The Flash update corrects several critical vulnerabilities in Flash versions 10.0.32.18 and earlier. Users should upgrade to the latest version - 10.0.42.34.


43. *December 8, Youngstown Computers Examiner* – (National) **Facebook iPhone app suffers a day of crashes.** Facebook’s iPhone app began crashing for many users Tuesday, with no explanation from Facebook for the crashes. The application would launch and appear for a few seconds, but completely close as it attempted to load users’ news feeds. The crashes do not seem limited to any particular model of iPhone. Users running the app on the iPhone 3G and 3GS were all reporting the problem, and multiple discussion topics on Facebook for iPhone’s fan page were growing rapidly as more and more users report the error. Traditional attempts to cure app crashes have not offered any hope. Uninstalling and reinstalling the app has not helped many, if any, users. Rebooting the iPhone does not seem to help matters, either. Changing wireless
networks does not seem to be a solution, either. The crashes are happening regardless of how the iPhone is connected - WiFi, 3G, or EDGE. Most users are speculating that the crashes are caused by a system malfunction in Facebook’s servers, but the social networking site has not issued any official notice of the glitch.

44. December 8, The Register – (International) Koobface worm dons tinsel to snag seasonally-affected marks. Miscreants have begun using Xmas-themed lures to push the Koobface worm. The attack starts off with a post from fake Facebook profiles that point to supposed video clips. Following these links takes users to a fake YouTube site that claims users need to install a Flash Player update to watch these “movie clips”. In reality this supposed codec is the download component of the Koobface worm, an approach seen several times over recent months with previous versions of the worm. This time around the fake video poses as a message from SantA, a tactic cynically designed to appeal to children, instead of the usual run of smut or celebrity-themed flicks. The Koobface worm is not the first item of badware to cloak itself in a seasonal guise this year. Trend reports that it detected somewhat prematurely Xmas-themed spam running as far back as September.
Source: [http://www.theregister.co.uk/2009/12/08/xmas_koobface/](http://www.theregister.co.uk/2009/12/08/xmas_koobface/)

45. December 8, BitDefender – (International) BitDefender releases ‘Conficker — One Year After’ whitepaper. BitDefender announced on December 8 the release of ‘Conficker « One Year After’, a whitepaper detailing the Conficker worm’s first appearance in November 2008, the damage it has done, and predictions on how it will spread in 2010. Conficker is a well-written piece of malware that has the potential to cause a lot of damage with the intelligent manner in which it updates itself. BitDefender’s ‘Conficker « One Year After’ whitepaper also provides tips on how readers can keep their systems protected from the worm. Conficker (a.k.a. Downadup or Kido) is a network worm that takes advantage of vulnerabilities in Microsoft’ Windows’ in order to spread. Its main purpose is to compromise as many machines as possible by exploiting a vulnerability in Microsoft Windows RPC Server Service, described in the Microsoft Security Bulletin MS08-067. The vulnerability allows a cybercriminal to remotely execute code onto an unprotected machine. Since its inception, there have been numerous variants of the Conficker worm. Some variants use the exploitation of the Autorun function for removable drives and media (such as USB portable storage devices) to spread, while others take advantage of weak passwords to infiltrate networks. Another variant disables Microsoft Windows Update and blocks access to the majority of internet security vendor Web sites, which means users cannot access automatic or manual security updates. BitDefender researchers predict that Conficker will become an even bigger threat in 2010 by the corruption of defensive systems, distributed denial of service, pay-per-click system abuse and fraud, key logging, and spamming.
46. December 8, Nextgov – (National) **Cyberattacks against critical U.S. networks rising at a faster rate.** The number of cybersecurity attacks against computer networks that operate the nation’s critical infrastructure such as transportation systems and water treatment and power plants, has increased dramatically, mostly because these industries rely on legacy technologies that do not protect systems from sophisticated attacks. In the third quarter, 11 cyber incidents were added to the Repository for Industrial Security Incidents, a database of cybersecurity attacks that have or could have affected systems that operate major industrial operations in the United States. These key networks are known as Supervisory Control and Data Acquisition systems. The owners and operators of industrial plants maintain the database. For all of 2009, industries have added 35 incidents to RISI, representing more than 20 percent of the 164 incidents recorded since 1982. The total number of incidents in the database could increase 37 percent this year if trends continue at the current rate, according to RISI’s third-quarter report, which was released on November 30. Malicious software such as viruses, worms and Trojans were the cause of most cyberattacks, according to the report. Incidents involving unauthorized access or sabotage by people working for the company such as disgruntled former employees or contractors also increased. Old technology presents a particularly difficult problem to solve. While most computer systems are upgraded every three to five years, control systems typically remain operational for up to 20 years, said the director of control systems security at the Homeland Security Department. These old systems were not developed to function in a networked environment or combat the onslaught of cyberattacks.


For another story, see item **14**

**Internet Alert Dashboard**

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: [http://www.us-cert.gov](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](https://www.it-isac.org)

[Return to top]

**Communications Sector**

47. December 9, Fairbanks Daily News Miner – (National) **$6.8 million gift allows UA to backup data center.** For more than a decade, officials at the University of Alaska have been quietly hoping that nothing goes horribly wrong at the Butrovich Building. The data center for the UA system is stored in the West Ridge administrative building, and officials say a disaster — either natural or man-made — would cripple record-keeping for payroll, student loans, personnel records and more. “We’d be out of business,” said the UA executive director of infrastructure technology services. On December 8, UA announced a gift from Alaska Communications Systems that should alleviate the problem by the end of 2010. The telecommunications company has agreed to donate
use of a data center in Oregon to back up UA’s record-keeping system. The gift, which will be spread throughout the next five years, is worth an estimated $6.8 million. “It fixes what is probably our single biggest vulnerability at the university,” said the UA President. Backup data tapes are made each day and stored off-site, but the use of the ACS facility will allow UA to continue online business operations that would otherwise be disrupted in the wake of a major disaster. Online functions will be able to resume within an hour once the new system is in place, said a UA spokeswoman. $1.5 million worth of hardware to make the new system work, but that the service itself, including maintenance, will come at no cost to UA. The gift agreement lasts until 2015.

Source: http://newsminer.com/pages/full_story/push?article--6-8+millon+gift+allows+UA+to+backup+data+center &id=5050104--6-8+millon+gift+allows+UA+to+backup+data+center&instance=home_news_window_left_top_4

48. December 9, ComputerWorld – (National) AT&T moves closer to usage-based fees for data. AT&T is moving even closer to charging special usage fees to heavy data users, including those with iPhones and other smartphones. The CEO of AT&T Mobility and Consumer Markets on December 9 came the closest he has so far in warning about some kind of use-based pricing. He spoke to attendees at a UBS conference in New York. “The first thing we need to do is educate customers about what represents a megabyte of data and...we’re improving systems to give them real-time information about their data usage,” he said. “Longer term, there’s got to be some sort of pricing scheme that addresses the [heavy] users.” AT&T has found that only 3 percent of its smartphone users — primarily iPhone owners — are responsible for 40 percent of total data usage, largely for video and audio, the CEO said. Educating that group about how much they are using could change that, as AT&T has found by informing wired Internet customers of such patterns.

Source: http://www.computerworld.com/s/article/9142012/AT_T_moves_closer_to_usage_based_fees_for_data?taxonomyId=1

49. December 8, KOAT 7 Albuquerque – (New Mexico) Communications glitch closes Rio Rancho schools. A communications glitch — not weather — gave Rio Rancho students a day off on December 8. “It was the fact that we had no communication with the buses that caused us to have initially a two-hour delay and because it was still down, we decided to close schools for the day,” said the Director of transportation for Rio Rancho Schools. Officials with the communications company said the driving snow and fierce wind ripped the antenna off the communications tower on top of Sandia Crest — and tossed the antenna about 200 feet on December 7. With such dangerous conditions outside, the district did not want to operate buses without communication. School district transportation officials bought cell phones on December 8 for bus drivers who did not have them. As for the antenna, officials said it is up and running for December 9.

50. *December 8, Associated Press* – (National) **FAA examines reliability of communications network.** The Federal Aviation Administration said Tuesday it is forming a panel to examine the reliability of a telecommunications network that broke down last month, snarling air traffic across the country. The November 19 episode — which resulted in delays of 819 flights and forced air traffic controllers to manually enter flight information into computers — was unacceptable, a FAA Administrator said in a statement. He said the agency needs to understand what happened so that it can prevent further incidents. “This panel is going to take a hard look at every part of the (telecommunications) operation,” he said. “We have an extremely reliable system, but we need to have the confidence that problems can be solved quickly and efficiently so our air traffic controllers and aircraft operators have the tools they need and travelers aren’t inconvenienced.” FAA said at the time that the incident began with the failure of a single circuit board in a router. A backup circuit board also failed. As a result, misinformation was sent to FAA computer centers near Atlanta and Salt Lake City. It was four hours before the glitch was fixed.

Source: [http://www.google.com/hostednews/ap/article/ALeqM5jXrjvmqVYNm4O_i4ak6IuZMR6eS9CFA1280](http://www.google.com/hostednews/ap/article/ALeqM5jXrjvmqVYNm4O_i4ak6IuZMR6eS9CFA1280)

---

**Commercial Facilities Sector**

51. *December 9, KVIA 7 El Paso* – (Texas) **Cohen canopy crumbles under gusty winds.** Intense wind damage occurred in the Northeast and one major casualty was the canopy at Cohen Stadium. City Parks and Recreation officials said there are four large sections and two side sections that make up the canopy. Just before 8:30 a.m. Tuesday, two of the larger sections were ripped right off the strong winds. The canopy flew into the desert area on the ballpark’s north side. The wind was so strong that the metal frame holding the canopy was bent and twisted. According to ABC-7 archives, the canopy was supposed to withstand 100 mph winds and have a lifespan of 30 years. City officials said they have sent pictures and information to the contractor and are waiting for their assessment.


---

**National Monuments and Icons Sector**

52. *December 9, Merced Sun-Star* – (California) **Memorial vandalism suspect is in custody.** A man accused of desecrating the veterans memorial in Courthouse Park, Merced, California has been taken into custody. The 18-year-old man was arrested by law enforcement in Norwalk on December 3. He was extradited from Los Angeles County and booked into the Merced County Jail on suspicion of vandalism Tuesday, according to a detective from the Merced Police Department. Police believe the man scrawled a graffiti message on the memorial around November 13, and police made a
report of the damage on November 16. The graffiti was written on the World War I memorial with a black paint marker. The graffiti message was about 8 inches long and 5 inches tall. The detective said volunteers with the Merced Community Action Network tried exhaustively to remove the marks but a large black stain from the graffiti still remains. Replacing the granite stone completely would cost $4,300, according to an estimate from the city’s parks and recreation department.
Source: http://www.mercedsunstar.com/local/story/1217623.html

53. **December 9, Herald Denver Bureau** – (Colorado; Wyoming) **Forest Service to spend millions to fight bark beetle outbreak.** The federal government will spend $30 million to protect against dead and falling trees in Rocky Mountain forests, the U.S. Agriculture Secretary announced Tuesday. However, Southwest Colorado’s spruce forests are not likely to see any of the money, because the bigger emergency is in the lodgepole pine forests of northern Colorado and southern Wyoming, a regional forester said. Colorado leaders have been clamoring for years for more federal help with the bark beetle outbreak, which has killed 2.5 million acres of lodgepole forests. The $26 million is the most significant infusion into the Forest Service’s Rocky Mountain region since the outbreak began. The money will not halt the beetle outbreak. Instead, much of it will be used to clean the mess left by the beetles. Lodgepole pines tend to tip over seven to 10 years after they die, and foresters are reporting more of the trees falling on roads and trails. They worry that falling trees will snap power lines, cut fences or even land on people.
Source: http://durangoherald.com/sections/News/2009/12/09/Forest_Service_to_spend_millions_to_fight_bark_beetle_outbreak/

**Dams Sector**

54. **December 9, WCTV 11 Tallahassee** – (Florida) **Plans to change dam brings fears of worse flooding.** A controversial dam project in Tallahassee is grabbing the attention of Leon and other surrounding County Commissioners. The Jackson Bluff Dam is owned by the city of Tallahassee but it affects people who live all along the Ochlockonee River. On Tuesday afternoon, Tallahassee officials presented plans to makes changes to the dam. But residents along the Ochlockonee say these changes will cause more severe flooding than what happens now. “There was no public input in the design of the project. We were simply informed of what the project was so we had no say in how that we were going to be affected,” says a resident who owns property along the Ochlockonee. “We’re certainly taking all the comments that are being raised by the citizens and the downstream and upstream governments into account and seeing if we can make design modifications or operational changes,” says the City of Tallahassee Power Production manager. County Commissioners from Liberty and Franklin Counties also voiced concerns about changes to the Jackson Bluff dam and how it will affect the residents in their counties. Structural changes to the dam are set to begin in
the Fall of 2010.

55. December 8, Dallas Morning News – (Texas) Potential Trinity River levee breach could flood outskirts of Combine. Combine, Texas, officials warned residents Tuesday of a potential breach of a Trinity River levee that could flood a portion of the town’s southern outskirts. The fire chief said at a community meeting that residents who live near the earthen Bois d’arc levee near Dawson and Harlan roads are not in immediate danger unless there is a considerable rain. “We’re going to have to have a week’s worth of heavy rain or eight inches in one night,” he said. Volunteer firefighters met with 11 homeowners near the river last week to warn them of the breach. He said there is a taxpayer levee district that manages and maintains the levee, but that board’s directors resigned several months ago for unknown reasons. The levee, built in 1918, has undergone several minor improvements, including one two years ago. Combine is near the Dallas and Kaufman county lines.

56. December 8, KHOU 11 Houston – (Texas) Texas City Dike closure hits businesses hard. The Texas City Dike was not built to serve as a fishing pier or recreation area. But in the 74 years since it was built, the dike turned into more than just a way to protect the Texas City Ship Channel. Boat ramps, fishing piers, and bait camps lined the shores of the 5-mile-long dike, and the beach area on the east shore was a popular spot for locals who wanted to avoid the beaches in Galveston. Hurricane Ike changed all that, destroying all the bait camps on the dike and the fishing pier on the dike’s end, and damaging the boat ramps, including the Yarbrough ramp, the third-busiest boat launching site on Galveston Bay. For the business owners who operated those bait camps, fishing piers, and even a snow cone stand and driving range on the dike, the inability to get the dike repaired and reopened before next fall has been devastating. The mayor has said repeatedly the priority, after months of delay waiting on federal funds, will be to repair the dike. Even that will not be complete until the end of summer of 2010. When the dike returns and, if the city renews the leases, it will be up to the businesses themselves to find the funds to rebuild. Pre-Ike discussions about development of the dike and ideas of charging an entrance fee to help defray costs to maintain the pier are off the table until the repairs are done.
Source: http://www.khou.com/home/Texas-City-Dike-closure-hits-businesses-hard-78765337.html
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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421

Subscribe to the Distribution List: Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.

Removal from Distribution List: Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nice@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.