Top Stories

- The Associated Press reports that on Tuesday about two dozen people were sickened by fumes from hydrochloric acid at the Manchester Tank plant in Quincy, Illinois. The plant manufactures pressure vessels. (See item 9)

- According to the Associated Press, hundreds of thousands of swine flu shots for children have been recalled because tests indicate the vaccine doses lost some strength, government health officials said on Tuesday. The shots, made by Sanofi Pasteur, were distributed across the country last month and most have already been used. (See item 24)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SERVICE INDUSTRIES
- Banking and Finance
- Transportation
- Postal and Shipping
- Information Technology
- Communications
- Commercial Facilities

SUSTENANCE and HEALTH
- Agriculture and Food
- Water
- Public Health and Healthcare

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. December 16, Corpus Christi Caller-Times – (Texas) More than 11,000 Corpus Christi households lost power this morning. The load of households in Corpus Christi turning up their heaters Wednesday morning may have caused an electrical substation to go offline and knock out power for 11,455 customers, an American Electric Power (AEP) spokesman said. The Rodd Field substation at Saratoga Rd. and
Yorktown Blvd. shut off about 6:40 a.m., an AEP spokesman said. He says crews are moving the power load to two other substations before they can re-energize the Rodd Field substation. The power was estimated to be restored to the area about 9 a.m. Source: [http://www.caller.com/news/2009/dec/16/more-11000-corpus-christi-households-without-power/](http://www.caller.com/news/2009/dec/16/more-11000-corpus-christi-households-without-power/)

2. **December 16, WYFF 4 Greenville – (South Carolina)** Tanker crash shuts down S.C. road. A collision involving a gas tanker truck and a pickup truck sent thousands of gallons of fuel onto a Spartanburg County road. The spill and the wreckage forced emergency crews to close the road for the day. The Hot Spot tanker was upside down and leaking fuel on Southport Road. Spartanburg County Emergency Management said the tanker had just filled up at a terminal in Camp Croft. It was carrying 8,000 gallons of fuel; 6,000 in gasoline, 2,000 in diesel fuel. According to the Highway Patrol, at 7:20 a.m. the pickup truck was traveling south on Southport Road and the tanker was traveling north. Troopers said the pickup went to turn left onto South Avenue and ended up pulling in front of the tanker. The wreck damaged the pickup truck and caused the tanker truck to flip upside down. Both drivers suffered non-life threatening injuries. Three firefighters were taken to the hospital with respiratory irritation. Southport Road was closed between Highway 221 and Highway 56. Environmental crews and first responders setup containment dikes, which kept the fuel out of nearby waterways. The Department of Health and Environmental Control said the rain-soaked soil kept the fuel from sinking in. Foam was applied to the area around the truck to contain vapors and suppress the possibility of ignition. The Emergency Management official said the foam costs around $100 per gallon. Those who work around the accident scene said the intersection is very dangerous.


3. **December 16, KWES 9 Big Spring – (Texas)** Copper theft on the rise in the Permian Basin. Oil fields across all of West Texas are a little bit emptier, and thieves are nabbing everything from oil and gas equipment to copper wiring. Right now, just about all West Texas law enforcement have been busy hunting down burglars in oil fields, wind turbine sites, and even air conditioning companies. The Midland County Sheriff told NewsWest 9 that this is a daily battle. In Hobbs, police say the past two months have been flooded with oil field investigations. Ector, Andrews, and Ward counties say there are no major investigations right now. But when theft spikes, the FBI Task Force pitches in. Officials in Gaines County say about once every three days there is another burglary. It is pulling deputies off the streets and out to the oil fields. And on the evening of December 15, Martin County officials were on the hunt for crooks suspected of snagging $8,000 worth of copper wiring. Deputies say the two main reasons behind the theft are narcotics and angry employees who lost their jobs when the economy tanked. “People involved in this type of crime, they don’t stay in one location,” the deputy said. “They could be in Texas today, they could be in Colorado tomorrow.” That is why Texas became the springboard for the Energy Security Council, an organization that tracks down crooks even after they have crossed state lines.

4. *December 15, WFSB 3 Hartford* – (Connecticut) **Substation problem leaves 10,000 in dark.** A problem at a Waterbury substation left about 10,000 people in the dark the morning of December 15, Connecticut Light & Power (CL&P) officials said. Officials said the problem was reported at 11 a.m. after an equipment failure at the substation. Officials said they shut down the substation to reduce the risk of further damage to the equipment. The problem caused outages in Watertown, Waterbury, Middlebury and Woodbury. Kennedy High School in Waterbury dismissed students at noon because of the outage, and Westside Middle School was dismissing students at 1 p.m., school officials said. Officials at the Waterbury campus of Western Connecticut State University said its branch would be closed for the remainder of the day because of the outage. CL&P crews worked to repair the problem and power was restored to the area. Officials said they will launch an investigation into the cause of the problems at the substation.


5. *December 15, WTFV 5 Nashville* – (Tennessee) **Thieves steal copper from multiple Clarksville substations.** The Clarksville Department of Electricity (CDE) recently discovered that half of their substations had been pillaged by copper thieves. Crooks cut hundreds of feet worth of ground wire from five different substations, stripping utility poles from top to bottom. “We’ve estimated right now there is $20,000 worth of damage to repair,” said a CDE spokesperson. Officials said the copper thefts did not cause any power outages. While investigators are confident they will catch the thieves, doing so will not be easy. “Most of the substations are off the beaten path. They are not on the highway, so it will be a little more difficult to see them,” said a Clarksville Police spokesperson. Clarksville Police are asking residents to be on the lookout for unusual behavior at power substations.


Chemical Industry Sector

6. *December 15, KOMO 4 Seattle* – (Washington) **Truck slams into overpass on SR 167 near Sumner.** One person was injured in a crash involving a semi truck on State Route 167 on Tuesday night. Troopers said trouble began when the truck traveling north veered off the road and slid onto a roadside embankment at a high rate of speed. The truck flew forward and smashed into an overpass around 6:30 p.m. The impact sheared off the top of the vehicle’s cab and ripped off the tank, releasing the chemical stored inside. Troopers initially identified the spilled chemical as liquid nitrogen and took extreme caution, but later redefined it as carbon dioxide used to carbonate sodas. “We didn’t even go in and get the driver,” said a trooper of the initial response. “We didn’t know what we had. We did a worst-case scenario (response), evacuated about a quarter mile in every direction.” The truck driver, a 46-year-old Auburn man, was taken to Harborview Medical Center, where he is listed in critical condition. It is not known what caused him to veer off the road. The overpass bridge at 24th appears to be significantly damaged, but it is still safe to drive under it, a spokesman said. The
bridge, which sustained a foot and a half-long indentation from the crash, will remain shut down until the Department of Transportation can assess its safety.


Nuclear Reactors, Materials and Waste Sector

7. December 16, Reuters – (Arizona) APS Ariz. Palo Verde 2 reactor back at full power. Arizona Public Service’s 1,314-megawatt Unit 2 at the Palo Verde nuclear power station in Maricopa County, Arizona had returned to full power by early Wednesday from 55 percent power early Tuesday, the U.S. Nuclear Regulatory Commission said in a report. Operators took the unit off line over the weekend to replace a hot neutral bushing that was increasing the temperature on a main transformer.

Source: http://www.reuters.com/article/idUSN1626241920091216?type=marketsNews

Critical Manufacturing Sector

8. December 15, U.S. News and World Report – (National) Recall Alert: 2002-2003 Subaru Impreza WRX. Subaru has issued a recall on 2002 and 2003 models of the Subaru Impreza WRX in order to fix a problem with the vehicle’s fuel system that could set it ablaze. The New York Times reports that the recall was issued after receiving “944 complaints of either fuel leakage or the smell of gasoline including one report from Subaru about a fire.” Cars.com explains, “The cars are being recalled because of a potential fuel leak in the fuel delivery line where the line connects with a rubber hose. During cold starts in extremely cold temperatures, the likelihood of a leak increases. Obviously, given an ignition source, a fuel leak could start a fire.” According to the National Highway Traffic Safety Administration, the recall applies to all 2002 to 2003 models “originally sold in or currently registered” in the following low-temperature states: South Dakota, Nebraska, North Dakota, Minnesota, Idaho, Iowa, Montana, Colorado, Wisconsin, New York, Wyoming, Michigan, Alaska, New Hampshire, Vermont, and Maine.


9. December 15, Associated Press – (Illinois) Fumes sicken more than 20 workers at Quincy plant. Officials say roughly two dozen people were sickened by fumes from hydrochloric acid at a plant in the Mississippi River city of Quincy. All the workers affected Tuesday morning at Manchester Tank were taken to a hospital, though their injuries were not thought to be life-threatening. Most were later released from the hospital. A spokesman for Tennessee-based McWane Inc., which owns Manchester Tank, says an investigation is under way into what caused the accident. The spokesman says there was no actual spill of the acid, only a leak of fumes — perhaps from some
air-scrubbing equipment. Manchester Tank makes pressure vessels for the containment of propane, compressed air and chemicals.
Source: http://cbs2chicago.com/wireapnewsil/Fumes.sicken.more.2.1371776.html

Defense Industrial Base Sector

10. December 16, Aviation Week – (National) U.S. Marines may not wait for JLTV. The U.S. Marines are in active talks with industry for a lightweight vehicle that may supplant the Joint Light Tactical Vehicle (JLTV), according to the Commandant. He told reporters at the Pentagon December 15 that the JLTV is not only five years away, but is weighing in at 22,000 pounds, which he believes is too heavy for Marine Corps needs. Spearheaded by the U.S. Army and the Marines, the JLTV is intended as a Humvee replacement.

Banking and Finance Sector

11. December 16, Wall Street Journal – (International) Credit Suisse to pay U.S. $536 million in Iran probe. Credit Suisse Group, one of Switzerland’s biggest banks, said Tuesday that it expects to pay a $536 million penalty as part of a continuing U.S. investigation into how major Western banks illegally handled funds for Iran. Credit Suisse’s role in alleged illegal transactions with Iranian enterprises previously had been disclosed. But the size of the fine and the fact that the Swiss bank joins other banking companies in settling U.S. inquiries highlight how far-reaching and secretive money flows have been with Iran and others sanctioned by the U.S. An agreement by the Swiss bank to pay that amount now means that fines and penalties for banks investigated in the alleged transactions are in the $1 billion range. Credit Suisse, which said it is in “advanced settlement discussions” with state and federal U.S. authorities, said that while it already set aside money to cover a fine, it will now record a 445 million Swiss franc ($430 million) pretax charge in the fourth quarter. The bank reports those results on February 11, 2010. Credit Suisse said that it was in the settlement talks with the Manhattan District Attorney, the Justice Department, the Federal Reserve and the Treasury Department’s unit that enforces economic and trade sanctions.
Source: http://online.wsj.com/article/SB10001424052748704398304574598303234399682.html

12. December 16, Computerworld – (National) Mass. Supreme Court throws out lawsuit against BJ's over '04 data breach. The Massachusetts Supreme Judicial Court affirmed a lower court ruling dismissing a lawsuit brought against BJ’s Wholesale Club
by dozens of credit unions over a 2004 data breach. The court held that the credit unions could not seek restitution from BJs on their claims that the wholesaler had breached a third-party contract and had misrepresented facts about its compliance with payment industry security standards. The ruling on December 11 is similar to numerous others that have been handed down by courts recently and highlights the challenges that plaintiffs face in winning tort actions against companies that suffer massive data breaches. Just last week, a federal court in New Jersey threw out a shareholder lawsuit against Heartland Payment Systems that disclosed a major data breach in January. The court essentially said that the data breach by itself did not demonstrate Heartland’s lack of commitment to maintaining a high level of security. Framingham, Massachusetts-based BJs in March 2004 disclosed that hackers had gained access to systems that stored credit-card transaction data. The initial intrusion had taken place in July 2003, but the breach was not discovered until Feb 2004. In that time, the hackers responsible for the intrusion, who have since been arrested, accessed magnetic stripe data on more than 9 million credit and debit cards. BJs later admitted that the compromise stemmed from its failure to purge magnetic stripe data from its systems as it was required to under payment card industry security standards mandated by MasterCard and Visa. Credit unions and banks had to spend millions of dollars blocking and reissuing cards that were compromised in the breach. Many also had to deal with fraud arising from the use of the stolen card data.

Source:
http://www.computerworld.com/s/article/9142361/Mass._Supreme_Court_throws_out_lawsuit_against_BJs_over_04_data_breach

13. **December 15, Computerworld – (International)** Hackers are defeating tough authentication, Gartner warns. Security measures such as one-time passwords and phone-based user authentication, considered among the most robust forms of security, are no longer enough to protect online banking transactions against fraud, a new report from research firm Gartner Inc. warns. Increasingly, such measures are overwhelmed by online criminals looking to pillage bank accounts using valid login credentials stolen from customers, the report said. Going forward, banks need to quickly implement additional layers of security to protect their customers from falling victim to online fraud, said a Gartner analyst and the report’s author. Gartner’s warning comes amid a sharp uptick in fraud involving the exploitation of valid online banking credentials. In August, NACHA- the Electronics Payments Association issued an alert, warning members about attacks involving the theft of online banking credentials, such as usernames and passwords mostly from small- and medium-size businesses.

Cybercriminals used the stolen credentials to take over corporate accounts and initiate unauthorized transfers of funds via electronic payment networks, NACHA said in its warning. NACHA, with more than 11,000 financial institutions as members, oversees the Automated Clearing House (ACH) electronic payments network. Just a few days earlier, a similar alert was sent to members of the Financial Services Information Sharing and Analysis Center. The alert identified organized cybercrime groups in Eastern Europe as predominantly responsible for illegally siphoning millions of dollars off corporate accounts and sending the money overseas via popular money and wire transfer services.
14. **December 15, CNET News** – (International) **Virtual currency exchange to launch in 2010.** Beginning in the first quarter of 2010, social sites IMVU and MyYearbook will launch a virtual currency exchange allowing users from either service to exchange currency between the sites. Currency Connect is billed as a “cross property virtual currency exchange” system similar to how one would change U.S. dollars into euros if one were traveling in Europe. Users simply swap their currencies depending on what site they are on. Most still find it surprising that users would exchange real money for virtual money that can never be taken out of a specific site. It makes one wonder when a bigger payments vendor, like PayPal, will get into the game and offer more of a de facto universal virtual. It cannot be long before other social sites like Facebook join the fray. Ultimately, the site or currency with the most users is likely to be the one with the most users. This opens up an opportunity for other sites with large user bases such as Google and Yahoo to offer a currency program. If users are already joining multiple social-networking sites, there is no doubt that they are also using search engines and instant messaging. On the technical side, the service uses a simple set of REST APIs that implement the various checks and balances of the system. Security is maintained through tracking methods and server-to-server connections, which will initially limit how many sites can participate in the service. Again, a larger online service might have an easier time deploying a fully distributed, trusted service that did not require point-to-point connections.


---

**Transportation Sector**

15. **December 15, NBC Dallas-Fort Worth** – (Texas) **Gun hidden in teddy bear at DFW airport.** Transportation Security Administration (TSA) security screeners at Dallas/Fort Worth International Airport (DFW) late last month discovered a 9mm handgun hidden inside a hollowed-out teddy bear and stuffed into a passenger’s suitcase. The gun was in a passenger’s checked suitcase, so it was headed for the cargo hold and not the cabin of the plane. But the passenger was pulled off his international flight and arrested on an export violation of failing to declare the gun when he checked-in. The case highlights a problem screeners face every day. In the last year, TSA screeners at DFW have discovered more than 90 guns hidden in checked luggage and carry-on bags. In most cases, the agency does not believe the passengers were trying to harm anyone on planes. Some travelers simply forget they have weapons in their bag when they head for the airport. Guns hidden in bags constantly test the screeners, who look at about 30,000 pieces of luggage every day. In a room underneath the airport, specially trained technicians check images of bags as they pass through a high-tech scanner that looks for weapons and explosives.
Postal and Shipping Sector

Nothing to report

Agriculture and Food Sector

16. **December 16, Charlotte Observer** – (North Carolina) **Chicken plant cited in deadly ammonia leak.** Nearly six months after an ammonia leak at a Lumber Bridge, North Carolina chicken plant killed one worker and injured three others, state regulators have cited Mountaire Farms with nearly two dozen workplace safety violations. The new citations include 20 serious safety violations at the company’s chicken processing plant near Fayetteville. The proposed fines total $73,325. Among the citations: not ensuring that employees were properly fitted for respirators that were cleaned and disinfected. Labor Department officials said the penalties are not designed to make up for the injuries suffered or the loss of life. Mountaire Farms officials said in a statement that the safety of employees is a top priority.

17. **December 16, Associated Press** – (Iowa) **Fire at Iowa plant prompts health warning.** Officials say a fire at an abandoned meatpacking plant in Cedar Rapids prompted a health warning for neighbors about exposure to smoke. The warning was issued after the fire broke out at the former Farmstead Foods plant Tuesday morning. Residents living or working nearby were advised to stay inside to limit exposure to the smoke, which can cause eye irritation, coughs and sore throats. The Linn County public health director said part of the problem was not knowing what was in the building. A fire department spokesman said the building is unsound, and officials decided to let it burn because of safety concerns.
Source: [http://wcco.com/wireapnewsia/Fire.at.abandoned.2.1372907.html](http://wcco.com/wireapnewsia/Fire.at.abandoned.2.1372907.html)

For more stories, see items 18 and 20

Water Sector

18. **Unknown Publish Date, Olympian** – (Idaho) **Convicted Burley feedlot manager fined $5,000.** A southern Idaho feedlot manager convicted of violating federal drinking water...
laws and lying to an investigator was ordered Tuesday to serve four months of home detention and pay $5,000 in fines. The man, a manager at Double C Farms near Burley, has also been sentenced to three years of probation for illegally injecting fluids into the groundwater in 2005. He was convicted by a Pocatello jury in April of four felony counts of violating the federal Safe Drinking Water Act and corresponding state laws. During the trial, federal prosecutors argued that he used a series of pipes and irrigation wells to divert the fluids into the aquifer without permits. Prosecutors also tried to prove the fluids were tainted by manure and bacteria, making the crimes more harmful to the environment and eligible for stiffer punishment. But those claims were rebuffed during a hearing last month by a U.S. District judge who ruled the government failed to make a clear and convincing case the fluids were contaminated and that the man knowingly polluted the aquifer. Throughout the investigation and court case, the feedlot manager claimed he was not a polluter and was injecting nothing more than creek water. The judge rejected his motion for a new trial in September. But defense lawyers said they intend to appeal the conviction and argue that the federal government has no authority to regulate groundwater in Idaho and lacks jurisdiction to prosecute alleged violations. Concerns by state and federal officials emerged in May 2005 during a routine waste inspection of the 400-acre feedlot at Double C Farms. The inspection, conducted by an inspector with the Idaho Department of Agriculture, reviewed the irrigation wells, waste containment ponds and other waste and irrigation infrastructure. In January 2008, a federal grand jury indicted the man on charges of incorrectly installing backflow valves on the irrigation wells, which allowed water in the aboveground pipes to flow backward and into the wells.


19. December 16, KELO 11 Sioux Falls – (South Dakota) **Town of Miller without water.** The central South Dakota town of Miller is without water after a water main break. The Water Department superintendent says it is not known when the break will be repaired. He says fire protection is not a worry because fire trucks can hook right to the water tower if necessary. About 1,300 people live in the community. The start of school was delayed Wednesday because of the water problem.

Source: http://www.keloland.com/News/NewsDetail6371.cfm?Id=94078

20. December 15, Water Technology Online – (California) **Data shows major groundwater loss in Central Valley.** An unfortunate combination of drought, water exports, and excessive well pumping have severely depleted aquifers in California’s Central Valley, according to an article in the San Francisco Chronicle. A UC Irvine hydrologist presented the new satellite data from NASA, saying “Groundwater is being pumped at rates that are not sustainable, leading to declining water tables, water shortages, decreasing crop sizes and continued land subsidence.” Experts are concerned that the Central Valley, which produces 8 percent of the U.S. food supply, could see significant declines in production if current dry weather and groundwater pumping trends continue, the article noted.

21. December 15, Seattle Times – (Washington) 10 million gallons of raw sewage flow into Puget Sound off Magnolia. About 10 million gallons of raw sewage spilled into Elliott Bay on Monday night and Tuesday morning because of an equipment failure at the West Point treatment plant in Magnolia, Washington. The overflow, during a three-hour period ending at 1 a.m. Tuesday, happened when a switch in a tank malfunctioned, opening a gate and diverting all raw sewage arriving at the plant directly into Puget Sound. It took three hours to repair the switch so the gate would shut, said the plant manager. County officials have closed the nearby beach and are taking water samples to determine the overflow’s effects. The manager dispatched a crew of six to walk the beach Tuesday morning and said no waste was found on the beaches. King County notified the state Department of Ecology at 10:40 p.m. Monday of the recent spill, said the permit manager at Ecology for King County wastewater treatment. The malfunction happened when workers tried to engage a standby position for the emergency bypass gate at the front of the plant, which is routinely set during heavy rains. Instead, the switch malfunctioned and swung the gate open. The plant management team will be dissecting the event, the crew’s response, and maintenance practices. The county has five days to file a written report about what happened. Enforcement action, including fines of up to $10,000 per day and a regulatory order, could result from the spill.
Source: http://seattletimes.nwsource.com/html/localnews/2010513686_websewage15m.html

Public Health and Healthcare Sector

22. December 16, Detroit Free Press – (Michigan) Detroit medical data stolen after 2 security breaches. The personal medical information of an estimated 10,000 Detroiters — Social Security numbers and birth dates, included — has been compromised after two security breaches, city officials revealed Tuesday. In one incident, a thief broke into a vehicle of a health department employee in October, snatching a flash drive with information from birth certificates, said a department spokesman. The drive included information for residents in the 48202 and 48205 ZIP codes for 2008 and the first half of 2009. The employee had backed up information on her flash drive because information was being transferred between computers at work. Because the case remains under investigation, the department is not releasing details about the employee or any discipline she faces. Then, a thief broke into the immunization program office at the department’s Herman Kiefer Health Complex during Thanksgiving break. A desktop computer taken contained Medicare and Medicaid flu billing information of those who received a seasonal flu vaccine.

Wednesday. Hawaii is one of 11 states that achieved seven out of 10 key indicators of preparedness in the report, “Ready or Not? Protecting the Public’s Health from Diseases, Disasters and Bioterrorism. “The H1N1 flu outbreak has exposed serious underlying gaps in the nation’s ability to respond to public health emergencies and ... the economic crisis is straining an already fragile public health system,” reported the Trust for America’s Health and the Robert Wood Johnson Foundation. Hawaii scored points concerning the state laboratory’s ability to assure timely pick up and delivery of disease samples around the clock and having enough staff to work hours needed in an emergency like H1N1. Key infrastructure concerns highlighted by the study were lack of real-time coordinated disease surveillance and laboratory testing, outdated vaccine production capabilities, limited hospital surge capacity and a shrinking public health workforce. More than half of the states had experienced public health funding cuts and a 27 percent cut in federal preparedness funds since fiscal year 2005, “which puts improvements that have been made since the Sept. 11, 2001 tragedies at risk,” the report said.


24. *December 15, Associated Press* – (National) **Kids’ swine flu shots recalled; not strong enough.** Hundreds of thousands of swine flu shots for children have been recalled because tests indicate the vaccine doses lost some strength, government health officials said Tuesday. The shots, made by Sanofi Pasteur, were distributed across the country last month and most have already been used, according to the Centers for Disease Control and Prevention (CDC). The 800,000 pre-filled syringes that were recalled are for young children, ages 6 months to nearly 3 years. A CDC flu expert stressed that parents do not need to do anything or to worry if their child got one — or even two — of the recalled shots. The vaccine is safe and effective, she said. The issue is the vaccine’s strength. Tests done before the shots were shipped showed that the vaccines were strong enough. But tests done weeks later indicated the strength had fallen slightly below required levels. Young children are supposed to get two doses, spaced about a month apart. Health officials do not think children need to get vaccinated again, even if they got two doses from the recalled lots.


25. *December 15, Network World* – (Washington) **Avaya unified communications helps patients reach doctors by phone.** Two years ago, patients calling Group Health Cooperative in Seattle for medical advice had zero chance of getting their questions answered on the first call. Now that the cooperative has implemented unified communications, however, the chances are 71 percent. Back in 2007, in order to reach a care team, patients called a central number where someone would take a message, pass it on to the medical staff, and someone would call back when free. Today, patients of a clinic trialing the new system dial into an automated call tree, punch in their patient ID, indicate that they want to talk to the care team, and are routed to the appropriate
clinic where an actual doctor or nurse answers the phone. The new functionality required both a hardware and software upgrade to the cooperative’s Avaya phone system, and the upgrade has also enabled features with other potential benefits. For example, the customer service call center can get screen pops to access records needed to answer callers’ questions. And the group is piloting automated dial-out reminders to patients that tell them to take their medications or detail practices they should follow in order to address their particular ailments.

Source: http://www.computerworld.com/s/article/9142337/Avaya_unified_communications_helps_patients_reach_doctors_by_phone

26. December 14, Federal Computer Week – (National) VA puts hospital data on Data.gov. The Veterans Affairs Department (VA) is now putting raw data from its annual hospital report card online on Data.gov. VA is posting data on quality of care, patient satisfaction, availability of services, wait times, medical staffing, patient outcomes and other topics in a machine-readable format for the first time, according to a news release. VA issued its first public report card on patient quality and safety at Veterans Health Administration facilities in May 2008. The 1,400 hospitals in the system treat about 5 million patients a year. The latest hospital report card showed improvements in some categories. For example, 94 percent of veterans were immunized against pneumonia, an increase of 4 percentage points from 2008 numbers. However, women and minority veterans reported lower levels of satisfaction with the care they received. The White House launched the Data.gov Web site earlier this year to collect raw data from federal agencies and make it available to the public.


Government Facilities Sector

27. December 16, Associated Press – (International) Climate talks deadlocked as clashes erupt outside. Danish police fired pepper spray and beat protesters with batons outside the U.N. climate conference in Copenhagen on Wednesday. Hundreds of protesters were trying to disrupt the 193-nation conference, the latest action in days of demonstrations to demand “climate justice” — firm steps to combat global warming. Police said 230 protesters were detained. Hundreds of protesters marched on the suburban Bella Center, where lines of Danish riot police waited in protective cordons. Some demonstrators said they wanted to take over the global conference and turn it into a “people’s assembly.” As they approached police lines, they were hit with pepper spray.


28. December 16, KOVR 13 Sacramento – (California) Modesto school open day after fatal shooting. A Modesto elementary school will be open this morning with counselors on hand and extra security the day after a woman was shot and killed by police on the school campus. The shooting occurred at Catherine Everett Elementary
School on Mount Vernon Drive on Tuesday afternoon at around 2:00 pm, according to the Modesto Police Department. A woman, described as a white female in her 40s, had a butcher’s knife when she walked onto the school campus near a playground while children were playing and began hitting herself in the head with the knife and cutting herself. The school’s principal was able to distract the woman and protect the children for about three minutes until police officers arrived. When the first two police officers on the scene approached the suspect, she charged at them, according to the Modesto police department, forcing them to fire. The woman was taken to the hospital with a gunshot wound to the head and was later pronounced dead.

Source: http://cbs13.com/local/modesto.elementary.school.2.1371879.html

29. December 16, Washington Post – (National) House takes steps to boost cybersecurity. House leaders have asked the chamber’s security officials to implement a new cybersecurity training regimen for aides and take additional measures to protect sensitive information from potential hackers. After a six-week review prompted by the Washington Post’s disclosure of the ethics committee’s secretive deliberations, the House’s chief administrative officer recommended technology security updates that focused mostly on making staff aware of the security risks on the Internet. “Changes in security policies will make it clear that all sensitive House information will remain on House equipment at all times, it will be encrypted when stored on mobile devices and must not be transmitted on any public access system,” the chief administrative officer wrote in a letter to the House Speaker and the Minority Leader. A chief administrative officer undertook the review after a junior staffer took home a sensitive computer file that included a document naming every member of Congress the panel was investigating and updating most of the nearly three dozen investigations.


30. December 15, Mid Columbia Tri-City Herald – (Oregon) DEPOT: Mustard chemical weapon vapor detected. Traces of mustard chemical weapon vapor were detected on December 15 inside a storage igloo at the Umatilla Chemical Depot. The vapor was detected during routine monitoring of an igloo that was being heated to prepare for the incineration of mustard agent, likely next month. The vapor is suspected of leaking from a bulk container holding more than a ton of the agent as it thawed. Mustard agent freezes below 59 degrees. Usually vapors only are detected during the warm summer months as the chemical agent thaws, but the containers of mustard are so large that the containers are being warmed before being taken to the incineration facility. There was no danger to the public or environment, according to the Umatilla Chemical Depot. The igloos have a passive filtration system that prevents chemical agent vapor from escaping outside the structure and additional power filtration systems are installed if leaks are detected. The depot was closed because of icy roads Tuesday, but essential workers were still at the depot to deal with the leak.


31. December 15, U.S. Department of Justice – (Maryland) Former State Department employee sentenced for illegally accessing confidential passport files. A former
State Department employee was sentenced Tuesday to 24 months of probation for illegally accessing more than 65 confidential passport application files. The defendant, 28, of District Heights, Maryland, was also ordered by a U.S. Magistrate in the District of Columbia to perform 25 hours of community service. The defendant pleaded guilty on August 26, 2009, to a one-count criminal information charging her with unauthorized computer access.


32. **December 14, Associated Press** – (Minnesota) **Minnesota stops using Texas company to verify IDs.** The state of Minnesota says its agencies have stopped using a Texas company to verify the identities of new employees. Minnesota Public Radio reported that state officials are concerned that some 500 employees’ names, birth dates and social security numbers may have been accessible on the company’s Web site. State agencies paid Lookout Services of Bellaire, Texas, $1.50 a name to verify hires are authorized to work in the United States. The company runs employee data through the federal Department of Homeland Security’s E-Verify program, which confirms that a worker has legal status and a valid Social Security number.


**Emergency Services Sector**

33. **December 16, Associated Press** – (Massachusetts) **Fire truck that crashed had wrong parts.** A police report that was part of an investigation into a Boston fire truck crash that killed a veteran firefighter concluded that a fire department contractor installed “unsuitable” brake parts on the vehicle. The Boston Globe reported Wednesday that the report also said firefighters who were not qualified repeatedly adjusted the brakes in violation of national safety guidelines. The contractor replaced a brake chamber and pads on the ladder truck with “unsuitable” parts in spring 2008, which decreased stopping power significantly. The report said decreased braking power contributed to the brake failure January 9 when the truck careened down a steep hill and into a building, killing a firefighter. The district attorney announced last week there would be no criminal charges filed in the crash.


34. **December 16, WSAU 550 Wausau** – (Wisconsin) **Marathon County buys new emergency radios.** Marathon County, Wisconsin is changing a plan to buy emergency radios. The county board had been working with Tait-North America to upgrade emergency communications. Tait had been installing a series of repeaters and smaller antennas to improve rural coverage for emergency responders. Some fire departments claimed the Tait radios had coverage problems in remote areas. The company said the situation would improve as more antennas went up. Now the Marathon County Board has decided not to buy additional Tait radios. They instead will use federal stimulus
dollars to buy from Motorola. That company’s bid was about 18-thousand dollars higher, but many experts say the coverage and reliability of those radios is better. The upgrade to the county’s emergency communications system should be finished next year.

35. December 16, Palm Springs Desert Sun – (California) Police unveil 30-camera surveillance system. Desert Hot Springs, California police unveiled a public camera surveillance program Tuesday that the project engineer calls the first of its kind. “This is the first truly mobile, high-speed data network anywhere, and it’s definitely the first one for police vehicles for public safety,” said the chief technology officer with Lockheed Martin who said he consulted with other vendors. The $1.2 million system includes 30 cameras posted in public places and in 16 squad cars, most of which are now live. Dispatchers and officers will be able to monitor the cameras from not only their police station desktops, but also their laptops over a secure outdoor wireless network. In the squad cars, officers can use a touch screen to zoom around panoramic video of any of the sites, including the dash cameras of other officers.
Source: http://www.mydesert.com/article/20091216/NEWS08/912160315/1015/news08

Information Technology Sector

36. December 16, The Register – (International) Attacks spread malware with help from AppleInsider. Malware purveyors are exploiting web vulnerabilities in appleinsider.com, lawyer.com, news.com.au and a dozen other sites to foist rogue anti-virus on unsuspecting netizens. The ongoing attacks are notable because they use exploits based on XSS, or cross-site scripting, to hide malware links inside the URLs of trusted sites. As a result, people who expect to visit sites they know and trust are connected to a page that tries to trick them into thinking their computer is infected. “What’s interesting ... is the fact that it’s embedding iframes to redirect people,” an individual who is a senior security researcher at Zscaler, told The Register. “Typically, cross-site scripting is just that - it embeds script tags so it will embed javascript to run.” While it is not the most convincing attack ever seen, there is nothing to stop attackers from using the same technique to push web-based exploits, say the Adobe Reader zero-day attack that’s now circulating in the wild. The links work because appleinsider.com and the rest of the sites being abused fail to filter out harmful characters used in XSS attacks.
Source: http://www.theregister.co.uk/2009/12/16/rogue_av_attacks/

37. December 15, Computerworld – (International) RockYou hack exposes names, passwords of 30m accounts. Hackers breached a database at social networking application maker RockYou Inc. and accessed username and password information on more than 30 million individuals with accounts at the company. The passwords and
user names were stored in clear text on the compromised database and the user names were by default the same as the users Gmail, Yahoo, Hotmail or other Web mail account. RockYou did not immediately respond to a request for comment on the incident. In a statement sent to Tech Crunch, which first reported the breach, RockYou confirmed that a user database had been compromised that potentially exposed some “personal identification data” for about 30 million registered users. The company learned of the breach December 4 and promptly shut down the site while the problem was addressed, the statement said. Redwood City, California-based RockYou offers widgets that are used widely on social networking sites such as Facebook, MySpace, Friendster and Orkut. The company bills itself as a leading provider of social networking application-based advertising services with more than 130 million unique users using its applications monthly. The breach was discovered shortly after database security vendor Imperva Inc. informed RockYou of a major SQL injection error it had uncovered on a page on RockYou’s Web site. Imperva’s chief technology officer said the company learned of the vulnerability on RockYou’s Web site — and the fact that it was being actively exploited — as part of its regular monitoring of underground chat rooms.


38. December 15, CNET News – (International) **Facebook sues men for allegedly phishing, spamming.** Facebook has sued three men, alleging they used phishing techniques to gain access to Facebook user accounts and then sent spam from the compromised accounts. The lawsuit was filed on December 14 in federal court and named the three defendants and the companies associated with them, Choko Systems, Harm, and iMedia Online Services, according to a Facebook statement late on December 15. The defendants could not be reached for comment. A Facebook spokesperson was trying to find out what court the lawsuit was filed in. The lawsuit makes claims under the Can-Spam (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, the Computer Fraud and Abuse Act, the California Anti-Phishing Act and the California Computer Data Access and Fraud Act, according to Facebook. This is the latest legal action the social networking site has taken related to spam. In October, Facebook was awarded $711 million in a judgment against self-described “spam king.”

Source: http://news.cnet.com/8301-27080_3-10416265-245.html

39. December 15, DarkReading – (International) **Adobe Reader, Acrobat under zero-day attack.** Adobe’s Reader and Acrobat PDF applications have been hit by a new attack exploiting an unpatched vulnerability in the pervasive tools. So far the exploit has been used mostly in targeted attacks, but researchers say it could soon spread now that the cat is out of the bag. Adobe late December 14 issued a brief update about the as-yet undisclosed vulnerability in Acrobat Reader and Acrobat 9.2 and previous versions that’s being exploited in the wild. The vendor says it will issue a patch on January 12 in conjunction with its quarterly update schedule. “This vulnerability (CVE-2009-4324) could cause a crash and potentially allow an attacker to take control of the affected
system,” Adobe says. So far, Adobe and security researchers around the industry have been tight-lipped on details about the newly discovered vulnerability involved, but ShadowServer on December 15 said in its blog that the flaw resides in a JavaScript function in Acrobat and Reader. The trick is that the vulnerable JavaScript is hidden inside a “zlib stream,” which makes it difficult for security scanners to detect it, ShadowServer says. The flaw is found in 8.x and 9.x versions of the software, according to ShadowServer, and researchers are currently testing earlier versions for the bug as well. A senior research manager for Symantec Security Response says the exploit is similar to previous ones for Reader and Acrobat as well as for other client-side attacks. And like similar attacks, this one also recruits the victim to its botnet so that it can issue updates of its malware to the machine.


40. **December 15, ComputerWorld Canada – (International)** Symantec updates smart phone management suite. Symantec Corp. is rolling out a trio of updated products designed to secure and manage a user’s fleet of Windows smart phones across their lifecycle. In addition to a variety of mobile device management features, Symantec Mobile Management 7.0 will allow administrators to deploy applications and updates to the mobile fleet. The other two products include Symantec Network Access Control Mobile Edition 6.0 and Symantec Endpoint Protection Mobile Edition 6.0, which together will protect devices against malicious threats and unauthorized access to the corporate network or Microsoft Exchange server. The security giant said that while these products are only supported on Windows-based phones, the company is exploring Google Android and Apple iPhone solutions.


For more stories, see items 41 and 45

**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**

41. **December 16, IDG News Services – (International)** Rogue antivirus lurks behind Google Doodle searches. Malicious is the best way of describing many of the search results Google visitors got on December 15 when they clicked on Google’s front-page Doodle sketch, dedicated to Esperanto’s creator. It is the latest example of just how good scammers have become at manipulating Google search results. For months now,
they have followed Google’s Trending Topics section and then used search engine optimization techniques to push hacked Web pages up to the top of Google’s search results, security experts say. They do this by flooding hacked pages with keywords that are then recorded by Google’s search engine. Hackers have several ways of getting their code on legitimate Web sites — lately they have focused on stealing FTP login credentials, according to a research scientist with Barracuda Labs. The hacked sites that pop up when one clicks on December 15’s Google Doodle include a hair salon in New Jersey, an Texas tree company, and a science fiction group. On Tuesday, clicking on the illustration on Google’s front page commemorating the 150th anniversary of the birth of Esperanto’s creator generated an awful lot of malicious search results — taking visitors to dodgy advertisements or pages that tried to trick visitors into thinking their computers were infected and paying for fake anti-virus software. These results remained steadily in the top 5 to 10 search results for people who clicked on the Google doodle link on December 15, and often filled up about half of the first few pages of results, the research scientist said.


42. **December 15, IDG News Service** – (National) **AT&T offers new position on net neutrality.** The U.S. Federal Communications Commission (FCC) should back away from creating strict nondiscrimination rules requiring broadband service providers to carry all Internet content, because such net neutrality rules could hurt investment in networks, AT&T told the FCC on Tuesday. AT&T, a longtime opponent of strong net neutrality rules, nevertheless suggests in a letter to the FCC that “preserving the open character of the Internet is critically important to ensuring that all consumers have the opportunity to be creators of content and innovators from their homes or their garages.” However, the FCC should not prohibit broadband providers from entering into commercial agreements in which they provide “value-added” broadband services to some Internet companies, AT&T said.


43. **December 15, CNET News** – (National) **Wireless and broadcast industries begin spectrum debate.** The wireless and TV broadcasting industries faced off for the first time at a congressional subcommittee meeting on the Hill on Tuesday, setting in motion what could be a long drawn out battle over whether wireless spectrum should be reallocated and where the government will get this new spectrum. The president and CEO of CTIA, the wireless industry group, and a member of the National Association of Broadcasters were among the witnesses gathered before the House Energy and Commerce Committee’s Subcommittee on Communications, Technology and the Internet to discuss what the CTIA and the Federal Communications Commission (FCC) have called a looming spectrum crisis. The hearing comes just weeks after the CTIA ruffled broadcasters’ feathers when it filed comments with the FCC suggesting that some of the additional spectrum it seeks for wireless broadband could come from
unused TV broadcast spectrum. Broadcasters oppose giving up their spectrum. And some representatives for broadcasters say they don’t believe that there is a spectrum crisis.
Source: [http://news.cnet.com/8301-30686_3-10416093-266.html](http://news.cnet.com/8301-30686_3-10416093-266.html)

44. **December 15, V3.co.uk** – (International) **World’s first LTE transfer achieved.** Another LTE milestone was reached after ST-Ericsson and Ericsson announced they achieved the first successful transfer of a mobile broadband data call between a next-generation LTE network and an HSPA network. ST-Ericsson, a joint venture between ST-NXP Wireless and Ericsson Mobile Platforms, said it was the world’s first transfer between networks of this nature. The chief technology officer and strategy planning office with ST-Ericsson said the test was important to demonstrate that LTE could be flexible enough to allow users to move between LTE networks and existing 3G networks as necessary. “If you’re travelling, for example, and move into an area where there is no LTE coverage your connection will continue regardless by moving on to an available 3G network,” he said.

45. **December 15, CNET News** – (International) **Australia moves toward mandatory ISP filtering.** Mandatory ISP filtering legislation will be introduced in Australia around the middle of 2010, after which there will be a one-year period to implement and activate the filtering technology. The Australian federal government on December 15 announced it will introduce amendments to the Broadcasting Services Act, which will by 2011 require all ISPs to block refused-classification-rated material hosted on overseas servers. As part of the new legislation, the government intends to explore what additional process could be implemented around how Web sites are added to the government’s “Refused Classification” (RC) list. The obvious contender for the new RC list’s oversight is the Australian Communications and Media Authority (ACMA), which manages a list of locally hosted illegal content, and issues so-called “take-down” notices to local operators.

**Commercial Facilities Sector**

46. **December 15, Bakersfield Californian** – (California) **Supervisors hear details of harrowing tent collapse.** Inside the SpaceShip 2 after-party tent on December 7, about 1,000 celebrities, sheiks, princesses and international dignitaries were enjoying the vodka bar, the million dollar telescope and the afterglow of the unveiling of the world’s first commercial spaceship when wind became a security problem. The tent was rated for 70-knot winds and had no shielding from the north. Kern County sheriff’s deputies, Kern County firefighters and California Highway Patrol officers moved into the party as a public address system announced the evacuation. A deputy fire chief was on the scene and said the evacuation was orderly and safe and was completed in six minutes. As the dignitary-filled buses rolled away from the event, the wind peeled the tent like
an orange and sent the steel structure crashing onto the inflatable buildings next to it. “I believe there are people living today because of the decisions made that night,” the event supervisor said.

For another story, see item 27

[Return to top]

National Monuments and Icons Sector

47. December 15, Courthouse News Service – (Maryland; New York) 9/11 museum director says Web site hacked. A Maryland man hacked into the Ground Zero Museum Web site, deleted it and left a link that redirects Web surfers to a page that criticizes the museum, its founder claimed in Maryland Federal Court. The museum on West 14th Street in Manhattan showcases artifacts from Ground Zero of the September 11 terrorist attacks. The founder said the hacker collaborated with him to design the museum’s shopping cart page and revamp its gift shop page. The founder contends that after an argument over message board fodder on TripAdvisor.com, the hacker used his access codes to wipe out the site. In turn, it cost the museum revenue and decreased rankings in search engines. He claims the hacker also sent an email to the museum’s web host, A-1 Hosting Services, questioning the museum’s nonprofit status, prompting the company to cut off its donation of server space that hosts the Web site. Allegedly, the hacker restored the site after being contacted by law enforcement, but refused to restore the shopping cart and gift shop pages, which he said belonged to him. The founder also claims the hacker removed meta-tags from the site so search engines would not recognize it, and uploaded malicious files that would have allowed an attack on the servers. The founder and the Ground Zero Museum seek an injunction and punitive damages for defamation, conversion and copyright infringement.

[Return to top]

Dams Sector

48. December 16, Orangeburg Times Democrat – (South Carolina) Heavy rains result in spilling at Santee Dam on Lake Marion. Recent and ongoing rain in upstate South Carolina has increased inflows in the Santee Cooper lakes system, resulting in spilling operations at the Santee Dam on Lake Marion. Six primary spillway gates, part of the massive system of 62 spillway gates, have been raised four feet, resulting in a discharge of approximately 20,000 cubic feet (or 150,000 gallons) of water per second into the Santee River. Spilling is expected to continue until further notice, and information is updated each business day at the lakes information line. Spilling is a normal part of
Santee Cooper’s hydroelectric operations and can occur several times a year, although Santee Cooper has not spilled since March 2007 due to the recently ended drought. Source: http://www.thetandd.com/articles/2009/12/16/news/doc4b281f1e46a1b610836762.txt

49. December 15, Brewton Standard – (Alabama) **PowerSouth monitoring Gantt dam.** Due to heavy rainfall, PowerSouth Energy Cooperative continued a controlled release at Gantt and Point A dams. PowerSouth initiated its high water notification action plan at 6:30 p.m. Monday as the tail water below Point A dam exceeded 25 feet. PowerSouth controls the operation of the dams at Gantt and Point A lakes on the Conecuh River near Gantt, Alabama, which are subject to government-mandated water levels. Laws require PowerSouth to maintain 33.80 to 34.30 feet of depth at Gantt Lake, and 40 to 40.50 feet at Point A. As of 9 a.m. on December 15, pool levels were 34.01 feet at Gantt and 40 feet at Point A — both below normal levels. “We continue our controlled release at both dams,” said the Ingram PowerSouth communication manager. “With more rain expected over the next six to eight hours, it may be necessary to lower the lakes even more.” PowerSouth will continue to closely monitor conditions on the lakes and manage resources with extreme caution. Individuals with boats and other water-related equipment should always be alert to changing conditions on the lakes and be prepared to take necessary steps to protect their property. Source: http://www.brewtonstandard.com/articles/2009/12/16/news/doc4b27b0938c855227383000.txt
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.