Homeland Security

Daily Open Source Infrastructure Report for 12 January 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Associated Press reports that a powerful offshore earthquake rattled communities in far northern California over the weekend, cutting power to 36,000 customers, causing minor damage to homes and businesses, and sending about 30 people to emergency rooms to seek treatment for cuts and bruises from falling debris. (See items **4** and **56**)
- According to the Army Times, test versions of the Army's new plastic helmet have failed to protect against bullets and blunt force attacks. Officials would say only that all five of the test helmets, made by four companies, failed in either ballistic or nonballistic testing. (See item **12**)

Fast Jump Menu

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

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

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

FEDERAL and STATE
- Government Facilities
- Emergency Services
- National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *January 11, Galveston County Daily News* – (Texas) **Oil storage tanks overflow; spill contained.** Three crude oil storage tanks just outside the Galveston, Texas city limits overflowed on January 10, but the spillage was contained within levee walls and did not pose environmental hazards, authorities said. A nearby resident noticed the tanks

overflowing about 3:15 p.m. and called Houston-based Nordstrand Engineering Inc., which owns and manages the site, a Galveston County Sheriff's Office spokesman said. The resident could not get through to the company, so he called Santa Fe Fire and Rescue. The sheriff's office, railroad commission, and representatives from the Texas Commission on Environmental Quality also responded, the Santa Fe Fire and Rescue Chief said. Officials got in touch with a representative from Nordstrand who shut off the pumps. About 400 to 500 gallons of crude oil overflowed into the containment levees but did not spill onto the ground. Workers still were vacuuming the oil at 6 p.m. and will investigate the cause of the system malfunction Monday. Nordstrand employees told officials the company lost power a couple days ago but did not know if it was a factor in the tanks' overflow. Each tank can hold 400 barrels of crude oil. The well pumps about seven barrels of oil and 15 barrels of water a day.
Source: http://www.galvnews.com/story.lasso?ewcd=f2168fa7c3836eb4

2. *January 11, Associated Press and INFORUM* – (North Dakota) **Oil pipeline leak reported in NE North Dakota.** An oil pipeline leak spilled about 126,000 gallons of crude in Pembina County in North Dakota's northeastern corner. Enbridge Energy Partners LP operates the pipeline, and the company reported on January 10 the spill had been contained and was being cleaned up. A company statement says the spill was confined to the pipeline's property, and no water or wildlife have been affected. Enbridge says pipeline regulators and the company are investigating what caused the leak. It was first detected January 8. The pipeline runs from Cromer, Manitoba, to Superior, Wisconsin. Enbridge said oil that is normally carried on the pipeline is being rerouted, and the affected pipeline will probably be out of service through January 11.
Source: http://www.inforum.com/event/article/id/265458/

3. *January 11, Associated Press* – (Alabama; Florida) **Cold causes power outages in the South.** Southerners hungry for heat are causing power outages across the region that is gripped by record low temperatures. By mid Monday morning, Florida Power and Light had about 14,000 homes without power and 1,300 restoration workers in the field. A power company spokesman said Sunday and Monday set successive records for electricity demand. Families in Tampa and in North Miami were treated for smoke inhalation after trying to use barbecue grills to heat their homes. About 7,700 homes and businesses in south Baldwin County, Alabama lost power when electrical demand overloaded a relay station. Crews from Riviera Utilities fixed the problem, but the system went down again. The utility is asking customers to turn off unneeded devices to help prevent more blackouts.
Source: http://www.kgan.com/template/inews_wire/wires.national/3fd78c8f-www.kgan.com.shtml

4. *January 11, Associated Press* – (California) **Eureka damage at $14.3M from quake.** The city of Eureka says it has racked up at least $14.3 million in damages from a powerful earthquake that struck over the weekend off the coast of Northern California. Damage estimates are still being tallied Monday. The temblor, which hit offshore about 27 miles southwest of Eureka, sent about 30 people to emergency rooms but only one was seriously injured. Power outages were widespread, affecting about

36,000 customers initially, but a quick response restored electricity to all by early Sunday, said a spokeswoman for Pacific Gas & Electric Co. The utility company was surveying gas lines by helicopter and on foot. Ten problems with gas pipes were reported; by Sunday afternoon, two had been repaired, and crews were working on the rest. The company's former nuclear power plant outside Eureka suffered no damage. "Our crews worked very quickly," said a PG&E spokesman. "We practice for this type of event, this type of emergency. We have earthquake plans; they were put in place and went very smoothly."
Source: http://www.chron.com/disp/story.mpl/ap/nation/6809613.html
See items **56** and **59**

5. *January 10, Reuters* – (International) **Chevron cuts back Nigeria oil flow after attack.** Chevron said on January 10 that it had been forced to shut down 20,000 barrels per day (bpd) of crude oil production in Nigeria, a day after security sources said gunmen had attacked a pipeline operated by the U.S. firm. "Chevron Nigeria Limited ... confirms that there was a breach on its Makaraba-Utonana pipeline in Delta State, Nigeria on Friday," the major U.S. oil producer said. Security sources told Reuters on January 8 that unknown gunmen in the oil-rich Niger Delta attacked the pipeline. No group has claimed direct responsibility. "This attack was sanctioned by MEND, but did not involve our fighters," the Movement for the Emancipation of the Niger Delta, the main militant group operating in the region, said in a statement. The pipeline attack comes five days after four Chevron workers in Delta state were killed in a shooting incident involving the military, said a spokesman for the state government. Violence in the Niger Delta has subsided for the past few months after thousands of gunmen handed over their weapons and accepted an amnesty offer from the Nigerian president. Thousands of guns, grenades and rounds of ammunition were surrendered under the amnesty, but security sources said from the start that peace would only last if those who disarmed were quickly re-trained and found work. But progress has been slow.
Source: http://af.reuters.com/article/topNews/idAFJOE60903520100110?pageNumber=1&virtualBrandChannel=0

6. *January 8, Associated Press* – (International) **Police make arrest in Canada pipeline bomb probe.** An anti-energy industry activist convicted of bombing oil and gas wells a decade ago was arrested on January 8 in connection with the investigation into a series of pipeline bombings in northeastern British Columbia, his lawyer said. The man is being investigated on charges of extortion against EnCana Corp. A Royal Canadian Mounted Police inspector would not identify the man arrested as he has yet to be charged. He said prosecutors have not made a decision yet. About 30 officers were searching a farm in the western Alberta town of Hythe in connection with the case. The farm belongs to the suspect, the suspect's lawyer said. There have been six bombings of EnCana pipelines in British Columbia since October 2008, which caused only minor disruptions to pipeline operations. The suspect is well known in Alberta for his opposition to the oil and gas industry. He was sent to prison in 2001 and served two-thirds of a 28-month sentence for his role in earlier gas well bombings in Alberta. Two EnCana gas wells and one owned by Suncor Inc. were hit in 1998, and another blast

cratered a road leading to a Norcen Energy well site. Police previously had said they did not consider the man a suspect in the latest pipeline bombings. He wrote an open letter to the bomber last fall appealing for a halt to the attacks. His lawyer said the man believed he had been summoned to the meeting to offer assistance to police in their investigation.
Source: http://www.pennlive.com/newsflash/index.ssf?/base/business-53/126297789847240.xml&storylist=business&thispage=1

For another story, see item **58**

[Return to top]

Chemical Industry Sector

7. *January 9, Courier Express* – (Pennsylvania) **I-80 eastbound closed near Emlenton to clean up from acid-spill accident.** Because of the rough road condition on Interstate 80 eastbound between exit 42 (Route 38) and exit 45 (Route 478) in both Butler and Clarion counties, Pennsylvania, the eastbound lanes were closed on January 9-10 , according to PennDOT Engineering District 10. PennDOT, along with employees from Swank Construction, milled the road and shoulders to provide a level driving surface. The road surface was damaged recently when a truck hauling acid split open, dumping the substance onto the roadway.
Source: http://www.leader-vindicator.com/site/news.cfm?newsid=20401616&BRD=2758&PAG=461&dept_id=572984&rfi=6

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *January 11, Herald News* – (Illinois) **Fire reported at Exelon.** A small fire led to an "unusual event" alert Saturday night at Exelon's Braidwood Nuclear Generating Station. The communications manager said a fire was reported on a plant ventilation fan bearing at 7:51 p.m. "There were no injuries and no damage to the plant. Both units remained at full power during the event," he said. "The fire was extinguished in 16 minutes after the initial report of smoke in the area by the station's fire brigade and no offsite assistance was required." The "unusual event" was called off at 9:11 p.m.
Source: http://www.suburbanchicagonews.com/heraldnews/news/police/1984002,4_1_JO11_BLOTTER_S1-100111.article

9. *January 9, Rutland Herald* – (National) **Entergy to probe radioactive leak.** Tritium leaks have surfaced at more than a dozen nuclear plants across the country, including several plants owned by Entergy Nuclear, the owner of Vermont Yankee. On Thursday, Entergy Nuclear announced that a monitoring well on the banks of the Connecticut River showed low levels of the radioactive isotope tritium, 17,000 picocuries per liter,

when the reportable level is 20,000 picocuries, according to the Environmental Protection Agency. An Entergy Nuclear spokesman said a special team was assembled to investigate the contamination. The spokesman said no additional tests were done on Friday on the well, which is about 36 feet deep and about 30 feet from the Connecticut River. One of the first issues is to determine the frequency of the testing of the well and surrounding wells. The special team will develop a plan, set priorities and use expertise from other plants, the spokesman said. One of Vermont Yankee's sister reactors in the Entergy nuclear fleet, the FitzPatrick reactor in upstate New York, disclosed it had a tritium contamination problem on December 29. It reported levels of 984 picocuries per liter. According to a spokesman for the Nuclear Regulatory Commission, the first priority is trying to find the source of the radioactive isotope.
Source:
http://www.rutlandherald.com/article/20100109/NEWS02/1090351/1003/NEWS02

[Return to top]

Critical Manufacturing Sector

10. *January 9, WSBT 2 South Bend* – (Indiana) **Fatal blast at Portage steel plant under review.** Investigators are taking a "hard look" at safety at a northwestern Indiana steel mill following an explosion that killed one worker and injured four just weeks after another blast at the same plant injured eight workers, a state official said Friday. The workers apparently were caught in a blast of superheated steam Thursday night after water met with molten steel in the electric arc furnace at Beta Steel in Portage, the Indiana Occupational Safety and Health Administration Deputy Commissioner said. "We are fairly convinced it was a steam explosion," he said. The Portage fire department said one worker died at the scene and the others were taken to hospitals with steam burns. Their injuries were not life-threatening. The president of the International Longshoremen's Association Local 2038 said the two millwrights and two supervisors were investigating a water leak in the furnace when the blast occurred. He said the blast appeared to be "very different" from one that occurred in November, which blew out the side of the furnace. That explosion was fire-related, he said. "Right now we are operating under the belief these were distinct different problems that just happened to occur on the same furnace," the president said. He said the investigation was still in its early stages. The overall safety record at Beta Steel, which produces hot-rolled coil for steel service centers and tube and pipe manufacturers, is good.
Source: http://www.wsbt.com/news/local/81059727.html

11. *January 8, WDAF 4 Kansas City* – (Missouri) **Heavy snow causes evacuation at Missouri plant.** The weight of snow has caused the roof of a Kawasaki motor engine plant in Maryville, Missouri to buckle, prompting plant managers to send employees home early until it can be fixed. According to the plant manager, the buckling was first noticed the week of December 28. He says that contractors thought that they had it stabilized, but the storm on January 6 caused more problems. On January 7, he was forced to evacuate the plant's 950 employees. To fix the problem, Kawasaki is going to have to cut holes in the roof and let the snow fall inside. Contractors are expected to be

working through the weekend to fix the roof. Kawasaki hopes to reopen the plant January 11.
Source: http://www.fox4kc.com/wdaf-story-snow-plant-roof-010810,0,4081512.story

[Return to top]

Defense Industrial Base Sector

12. *January 10, Army Times* – (National) **New plastic Army helmets fail tests.** Test versions of the Army's new plastic helmet have failed to protect against bullets and blunt force attacks. Some prototypes could not stop bullets, others could not withstand blunt force, and some failed on both counts. Officials would say only that all five of the test helmets, made by four companies, failed in either ballistic or nonballistic testing. The nonballistic tests examined the impact of blunt force trauma to the helmets from blast waves, rolled-over vehicles and fragmentation. The failures have set the program back, postponing Army plans to field the new helmet this year. The plastic helmets, which the Army also plans to field, are made with an ultrahigh molecular weight polyethylene, which is used commercially in everything from artificial hip replacements to police body armor. The heavy-duty plastic works well in body armor, because the armor is relatively flat. It becomes vulnerable when molded into a more circular, helmet shape and is also harder to manipulate, a spokesman said. He declined to detail the prototypes' failures any further, citing "operational security" and "acquisition sensitive" material. However, he said all the companies will have to do "enormously better" to meet the requirements laid out by the Army and Marines. Once the plastic helmet is developed, the services plan to initially purchase 238,500 of them; the Army expects to field 200,000 of them.
Source: http://www.13wmaz.com/news/local/story.aspx?storyid=73425&catid=28

13. *January 8, Associated Press* – (Maine) **2 truckers arrested with guns at Maine Navy yard.** Police say two Pennsylvania truckers are facing charges they tried to bring concealed weapons into the Portsmouth Naval Shipyard in Kittery. The Maine State Police says the handguns were discovered during a routine inspection of the truck at about 6:30 Thursday morning. The vehicle was carrying welding supplies into the Navy base. Both men were released on bail after appearing in court Friday. A Maine State Police lieutenant says the two had permits to carry concealed weapons in Pennsylvania, but not Maine. He says the two worked for a small trucking company from Lancaster, Pennsylvania.
Source: http://cbs3.com/wireapnewspa/2.Penn.truckers.2.1413753.html

[Return to top]

Banking and Finance Sector

14. *January 11, Wall Street Journal* – (Washington; California) **Regulators seize bank, credit union.** Regulators seized a small bank and a tiny credit union, the first two failures in a year that is expected to bring the collapse of many more financial

institutions reeling from the economic downturn and other woes. The Washington State Department of Financial Institutions closed Horizon Bank, an 18-branch bank based in Bellingham, Washington. Its $1.1 billion of deposits and nearly all of its $1.3 billion assets were assumed by Washington Federal Savings and Loan Association, of Seattle. Washington Federal didn't pay a premium to assume the deposits. It also entered into a loss-sharing agreement with the Federal Insurance Deposit Corp. on roughly $1 billion of Horizon's assets. The FDIC estimates that the collapse of Horizon will cost the agency's deposit-insurance fund $539.1 million. Like many small U.S. banks, Horizon was hobbled by bad real-estate loans. Separately, regulators seized Kern Central Credit Union, Bakersfield, California, a three-branch institution that served farm workers and had a large concentration of auto loans. Self-Help Federal Credit Union of Durham, North Carolina, assumed Kern's $34.9 million in assets and all its liabilities. Self-Help has $75.2 million in assets and targets low-income, female, rural and minority borrowers.
Source:
http://online.wsj.com/article/SB10001424052748703535104574647141197555718.html

15. *January 11, Bank Info Security* – (National) **Phishing scheme spread to 3 more states.** Financial institutions in Georgia, Iowa and Indiana report being hit by the automated phone phishing attacks that have been striking institutions across the U.S. since early last fall. These latest attacks represent only some of the various fraud scams that increased more than 600 percent last year, according to the Anti Phishing Working Group's report. In Chickamauga, GA, a phishing scam targeted random residents on the day after Christmas. Calls made by an overseas scam artist told some Bank of Chickamauga customers that "Your debit card has been restricted" and directed them to call a 1-888 number to lift the restrictions on their card. Nevada, Iowa residents began getting calls on December 28 from a scammer posing as a credit union. Local police say a scheme to get people to give out banking or credit card information is making its way through every phone number in Nevada, Iowa. River Valley Credit Union alerted its members to the scam with a fraud notice on its home page. The phone scam also hit a credit union and a bank in Indiana over New Year's weekend. The phone phishing scam began on New Year 's Eve in the Hagerstown and Greens Fork areas, and bank executives predicted it could spread east. The Perfect Circle Credit Union, Hagerstown, IN says the scam was hitting 489 and 886 area prefixes. West End Bank, Richmond, IN and Perfect Circle customers are being asked in the phone call to enter their debit card numbers because they are being cancelled. The credit union has more than 8000 members and assets of $47 million.
Source: http://www.bankinfosecurity.com/articles.php?art_id=2058

16. *January 11, Bank Info Security* – (North Carolina; Florida) **ATM skimming incidents increase.** Reports of ATM fraud incidents continue to rise. Criminals hit ATMs in two states over the recent holidays to skim account numbers and PINs from customers in North Carolina and Florida, according to police. In Raleigh, North Carolina, 300 members of State Employees Credit Union had money skimmed from their accounts. The skimmer may have been placed at a gas station, say police. SECU is second largest

credit union in the U.S., with $18.4 billion in assets. Skimming devices are often color coordinated, making them difficult to spot on ATMs. Finding the skimming device on a gas pump is virtually impossible as it is often hidden on the inside. SECU officials say the recent thefts likely happened at gas stations — not by using ATMs. It is not yet clear if other banks or customers in the Raleigh area were affected. Police in Naples, Florida say a man who was suspected of placing a skimming device on an ATM at a Naples bank struck again at another Sun Trust Bank location. The same man is suspected of placing a skimming device on a Sun Trust Bank on November 12, then another one at a different Sun Bank on November 27, and then again on December 12. It is not known how many card numbers the man may have taken in the three acts, but several customers later reported fraudulent charges on their debit cards on the east coast of Florida. Sun Trust Bank is headquartered in Atlanta, Georgia and has assets of $189 billion.
Source: http://www.bankinfosecurity.com/articles.php?art_id=2059

17. *January 11, The Register* – (International) **Rogue phishing app smuggled onto Android Marketplace.** A phisher hoping to harvest bank login details managed to smuggle his app onto the Android app store. Malicious apps posted by Droid09 were quickly identified, prompting a warning to legitimate users and a ban for the VXer. The incident raises questions about whether a tighter vetting process is needed for the Android Marketplace. The rogue Android application posed as a legitimate banking applet, but was actually designed to trick users into handing over bank login details to fraudsters, an alert by credit union First Tech warns. The credit union, which said it was not targeted by the attack, doesn't even have an app for Android as yet. Android fans who downloaded any of Droid09's apps are advised to purge them from their phones before consulting their mobile phone firm for further advice. The incident happened in December, but became public after news outlets picked up on First Tech Credit Union's fraud alert on January 11.
Source: http://www.theregister.co.uk/2010/01/11/android_phishing_app/

18. *January 8, Reuters* – (National) **Task force to target bankers who crashed economy.** The U.S. attorney general said on January 8 a newly created interagency task force was focusing on financial fraud and targeting for possible prosecution bankers whose actions contributed to the financial crisis. Speaking at a civic group meeting in West Palm Beach, Florida, the attorney general said the task force, which was created by the U.S. President in November and met for the first time last month, would focus on fraud in mortgages, securities, economic stimulus programs and government bailouts. He said the Justice Department and the task force also were investigating banks and other financial institutions whose failure to follow laws and regulations were in part to blame for the most serious financial crisis the United States has faced since the Great Depression. The attorney general said the Justice Department was moving forward on more than 5,000 pending financial institution fraud cases and the FBI was investigating more than 2,800 mortgage fraud cases — up nearly 400 percent from five years ago. The purpose of the task force, led by the Justice Department, is to investigate and prosecute financial crimes and to try to deter future fraud. The task force replaced a similar one established by the last Administration in 2002 after corporate scandals such

as the collapse of Enron Corp.
Source: http://www.reuters.com/article/idUSTRE6073P220100108

19. *January 8, IDG News Service* – (International) **Mobile banking faces uphill battle in mature markets.** The mobile phone is turning into the platform of choice for banking in emerging markets. In developed markets, however, the phone has struggled to compete with existing payment methods, and the challenges aren't going away in 2010. Mobile banking services gained momentum in 2009 with rollouts in dozens of countries in emerging markets, including Brazil, Cambodia and Malaysia, and the pace will continue this year, according to a research director at Gartner's Mobile Devices and Consumer Services group. "[The rollout of services] will help the unbanked people of the world to get access to financial services and help improve their quality of living," said the director. For people in emerging markets, the mobile phone is in many cases their only means of access to financial services, the director said. Developed markets, on the other hand, have well-established banking and payment infrastructures, so the advantage of using the phone isn't that obvious, she said. Still, mobile banking services are rolling out in developed markets as well. For example, mobile phone retailer The Carphone Warehouse and Monitise, which has developed a platform for mobile banking services, have joined forces to launch the Mobile Money Network in the U.K. in the first half of the year. The network will then be rolled out in Europe and the U.S., according to Monitise. Carphone Warehouse will use the network to let consumers send money to friends and family, top up their prepaid mobile phones and use text messages to buy goods, the chief strategy officer at Monitise said.
Source:
http://www.computerworld.com/s/article/9143503/Mobile_banking_faces_uphill_battle_in_mature_markets

20. *January 8, IDG News Service* – (International) **Money for nothing? Virtual goods market takes off.** Social networking and multiplayer online games are fueling dramatic growth in hard cash earned from goods that exist only in the world of online make-believe, according to companies in that market gathered at the Consumer Electronics Show in Las Vegas. The hugely popular Farmville game on Facebook may be the killer app opening up the virtual goods market to a new and more adult demographic, the members of social networking communities. Indeed, in the fourth quarter of 2009 the percentage of Americans who had purchased a virtual good or service doubled to 20 percent, according to a survey by Playspan, which provides a digital goods commerce and micropayment platform. The bottom line for the virtual goods and services business, though, is making it easy to extract real-world money from a market where most transactions have a cash value too low for credit-card use to be practical. In many cases, users spend around $12 to load up on virtual currency, which they spend in increments of less than a dollar. The infrastructure to support micropayments is now maturing, said the marketing director of Offerpal. His company helps game and virtual world sites monetize an audience that ignores conventional banner ads. They craft offers where users engage with an advertiser online in exchange for virtual currency to spend in the game.
Source:

http://www.computerworld.com/s/article/9143538/Money_for_nothing_Virtual_goods_market_takes_off

21. *January 8, U.S. Department of Justice* – (Texas) **Nineteen indicted in massive cybercrime conspiracy.** A federal grand jury in Dallas returned a superseding indictment charging 19 defendants in a massive cybercrime conspiracy, announced the U.S. attorney of the Northern District of Texas. This indictment supersedes a September 2, 2009, indictment that charged nine of the defendants in the conspiracy. The following 19 defendants are each charged with one count of conspiracy to commit wire and mail fraud. The eight-count indictment also charges 15 of the defendants with fraud and related activity in connection with electronic mail and aiding and abetting. The indictment alleges that from March 2003 through July 2009, the defendants conspired to defraud various telecommunications companies, including AT&T; Verizon; XO Communications; SMARTnet VOIP; Waymark Communications; the lessors of properties at 2020 Live Oak, 2323 Bryan Street and 1950 Stemmons Freeway, in Dallas; various financial institutions; leasing companies and creditors, including Wells Fargo, AT&T Capital Services, and the credit reporting agencies; and various other service providers, such as power companies, insurance companies, air-conditioning companies, website developers, and others for goods and services amounting to more than $15 million.
Source: http://dallas.fbi.gov/dojpressrel/pressrel10/dl010810.htm

[Return to top]

Transportation Sector

22. *January 10, KOMO 4 Seattle* – (Washington) **Ice shatters plane windshield at 15,000 feet.** There were some tense moments for passengers on a Seattle-bound flight late Friday when a chunk of ice slammed into their propeller plane at 15,000 feet. The impact shattered the plane's windshield. "I was reading, and I heard a loud bang," said one passenger. "And then I started to get nervous because the windshield completely shattered. I saw that the windshield was completely smashed and there was no visibility whatsoever out of his line of view," she said." Once the plane landed, investigators used flashlights to try and figure out what cracked the aircraft's windshield. The running theory is that a chunk of ice at 15,000 feet caused the impact.
Source: http://www.seattlepi.com/local/414047_iceplane10.html?source=mypi

23. *January 10, CNN* – (Ohio) **Power back on at Cleveland airport.** The lights were back on at Cleveland, Ohio's largest airport Sunday afternoon after a transformer explosion cut power at terminals for more than seven hours, an airport spokeswoman told CNN. About 800 travelers were stranded Sunday morning when Cleveland-Hopkins International Airport lost power at 6:50 a.m., a spokeswoman said. Terminals went dark and air traffic ground to a halt, but the control tower, runways and taxiways remained lit by backup generators, she said. The lack of power at terminals made it impossible to check in or screen passengers. Travelers remained calm and waited for some time, but many gave up and left, not knowing when operations would resume. All

power was restored by 2:30 p.m., and crews were checking that no cold-sensitive equipment was damaged and that all systems were running smoothly, the spokeswoman said. The transformer exploded after road salt swept into the air gradually corroded power lines.
Source: http://edition.cnn.com/2010/TRAVEL/01/10/cleveland.airport.outage/

24. *January 10, WPIX 11 New York* – (New Jersey) **Emergency landing at Newark airport.** A United Airlines flight made an emergency landing at Newark Liberty International Airport Sunday, after some of the plane's landing gear failed to function. A spokeswoman for the Federal Aviation Administration said the left side landing gear failed to deploy, while the right side and nose gear appeared to be working fine. The malfunction created a bumpier-than-usual landing. No injuries were reported. The Port Authority of New York and New Jersey said all 53 people aboard Flight 634 from Chicago got off the plane safely. It is still unclear what caused the malfunction. Investigators were inspecting the plane Sunday in search of answers. Newark Airport was closed for about 20 minutes, before two of its three runways reopened after the plane landed.
Source: http://www.wpix.com/news/local/wpix-newark-emergency-landing,0,1873392.story

25. *January 9, CNN* – (Colorado) **Fighter jets scrambled again because of unruly airline passenger.** In the second such incident in three days, fighter jets escorted a diverted commercial flight on Friday after an unruly passenger caused alarm onboard. The military sent up two F-16s in response to reports of an unruly passenger aboard AirTran Flight 39, the North American Aerospace Defense Command said in a statement. The passenger had become belligerent and refused to leave the restroom, an airline spokesman told CNN on Friday. The passenger appeared to be intoxicated, he said. NORAD dispatched the fighters at 1:44 p.m. ET, escorting the aircraft to a safe emergency landing in Colorado Springs, Colorado, officials said. The passenger was detained there and FBI agents from Denver, Colorado, were called to question passengers.
Source: http://www.wibw.com/nationalnews/headlines/81069172.html

26. *January 8, Wired* – (National) **Crack new scanner looks for bombs inside body cavities.** Even scanners using either millimeter wave or backscatter X-ray imaging might not have caught the terrorist who nearly brought down Northwest flight 253. Which is why one company is trumpeting a sensor that can supposedly "detect substances such as explosive materials hidden inside or outside of the human body." It is called Diffraction-Enhanced X-ray Imaging or DEXI, which employs proprietary diffraction enhanced imaging and multiple image radiography. Rather than simply shining x-rays through the subject and looking at the amount that passes through (a like conventional x-ray machine), DEXI analyzes the x-rays that are scattered or refracted by soft tissue or other low-density material. Conventional x-rays show little more than the skeleton, but the new technique can reveal far more, which makes it useful for both medical and security applications. The company has already demonstrated the technology with a unit originally designed for imaging small animals. The next stage is

a human-sized unit, which is being "finalized for extensive testing."
Source: http://www.wired.com/dangerroom/2010/01/crack-new-scanner-finds-explosives-inside-body-cavities/

27. *January 8, Bloomberg* – (Massachusetts) **De-icing fluid is blamed for smoke on Delta Boston flight.** Smoke in the cabin of a Delta Air Lines Inc. plane that briefly shut Boston's Logan airport probably was caused by de-icing fluid, according to the regional partner that operated the flight. The fluid "may have been applied near some inlets and created a smell of smoke on board," a spokesman said Friday in a telephone interview. All 25 passengers and 3 crew members on Delta Flight 6409 evacuated safely through the main cabin door and were re-booked on other planes, he said. The aircraft was to fly to Columbus, Ohio. The incident happened at 10:30 a.m. and caused takeoffs and landings to be halted for about 16 minutes, said an airport spokesman.
Source: http://www.businessweek.com/news/2010-01-08/de-icing-fluid-is-blamed-for-smoke-on-delta-boston-flight.html

28. *January 8, KDLH 3 Duluth* – (Minnesota) **Duluth airport evacuated after unattended bag found.** An unattended bag at the Duluth International Airport on Friday caused an evacuation. Officials say around 11:30 A.M., airport security found an unattended bag outside a screening area. "A group of people together, stopped in to use the restroom—had a bunch of bags—grabbed most of them, unfortunately not all of them," said a security officer with the Duluth Airport Authority. After no one claimed the bags, officials made the determination to evacuate the terminal as a precaution. After no harmful content was found in the bag, the airport reopened and the bag the owner of the luggage was located, but not before planes were affected. "There was one arriving flight delayed, two departing flights delayed—none canceled," said the spokesman. Airport officials would not comment when asked whether the bag's owner will face charges.
Source: http://www.northlandsnewscenter.com/news/local/81051907.html

For more stories, see items **2**, **4**, **5**, **6**, and **7**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

29. *January 11, Associated Press* – (Florida) **Even fish can't escape Sunshine State's cold.** Freakish cold weather continued to grip the southern Florida, with snow flurries spotted around Orlando and a record low set for Miami. About 100,000 tropical fish being raised on a fish farm in South Florida could not bear the cold. The owner of

Breen Acres Aquatics in the small town of Loxahatchee Groves just north of Miami, said temperatures dropped below 30 degrees overnight, leaving ice on his 76 ponds. The National Weather Service issued a hard freeze warning for South Florida from Sunday night to Monday morning. A freeze watch will continue through Tuesday. Northern Florida residents will feel temperatures drop to the lower 20s and mid-teens.
Source: http://www.msnbc.msn.com/id/34796151/ns/weather/

30. *January 10, Food Safety News* – (National) **FSIS sets pathogen standards for poultry.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) has developed new pathogen reduction performance standards for control of Salmonella and Campylobacter in chilled carcasses at young chicken (broiler) and turkey slaughter establishments that are eligible for agency verification sampling. In the past, FSIS has had standards for Salmonella but not for Campylobacter. The President's Food Safety Working Group made these recommendations for new standards to reduce the prevalence of disease-causing bacteria, specifically Salmonella and Campylobacter, in poultry. The new performance standards are based on the analysis of data from recent FSIS baseline sample collection programs for young chickens and turkeys. In the very near future, FSIS will issue a Federal Register notice that will provide specific details concerning the new standards. FSIS has set a goal that 90 percent of covered establishments will meet the new standards for Salmonella bacteria by the end of 2010. The new Salmonella performance standards will limit the number of positive samples that are acceptable in a defined set, as compared to past standards. The new Campylobacter standards will also limit the number of positive samples that are acceptable in a defined set.
Source: http://www.foodsafetynews.com/2010/01/fsis-sets-pathogen-standards-for-poultry/

[Return to top]

Water Sector

31. *January 11, Shreveport Times* – (Louisiana) **Shreveport residents asked to limit water usage.** Shreveport's Director of Operational Services on January 10 issued a request asking all residents to conserve water usage on January 10 and 11. The request came after the number of private water line breaks at residential and business facilities and is culminated with the water main blowouts the city is experiencing. "Since the thaw today we are seeing that our water demand has gone up to almost 55 million gallons per day versus our normal water usage this time of the year which is around 35 million gallons per day," he says. He says high demand normally would not be a problem since Shreveport's capacity is 90 million gallons per day, but the construction project at Amiss Water Purification Plant has forced the pumping at and over capacity. Officials are seeing low water pressure in parts of the city, mainly north and south Shreveport. "For the remainder of the day and throughout the day tomorrow, I am issuing an urgent request that all residents and businesses conserve their water usage and only use sparingly," he says. "We will have crews out for the rest of today and tonight repairing our water mains and ask that citizens comply with this conservation

request and bear with us until repairs are completed and our pressures are back to normal."
Source: http://www.shreveporttimes.com/article/20100111/NEWS01/1110312/1060

32. *January 11, Associated Press* – (Mississippi) **Jackson mayor, Miss. governor declare emergencies in Jackson over water outage.** The mayor of Jackson has urged residents to conserve water as city crews work on repairs to as many as 70 water lines that have broken since subfreezing temperatures of the past week. He says the breaks have caused the water system to lose pressure. He has extended the precautionary boil water alert for the entire city. He says crews will work over the next several days to bring the system back up to full capacity. Also Monday, the governor of Mississippi issued a state of emergency, closing state offices and sending nonessential workers home. Offices were to reopen Tuesday, unless otherwise notified. Jackson schools and Jackson State University closed as did some businesses. Also, there was no water at the state Capitol as lawmakers returned for the second week of the 2010 Legislative session. A water main busted overnight.
Source: http://www.wreg.com/news/sns-ap-ms--jacksonwateroutage,0,6184787.story

[Return to top]

Public Health and Healthcare Sector

33. *January 11, USA Today* – (Louisiana; National) **Katrina negligence lawsuit has implications for all hospitals.** A law suit prompted by the death of a woman who was on a respirator at Pendleton Memorial Methodist Hospital in New Orleans may have nationwide implications. The lawsuit alleges that negligence of the hospital's staff caused the woman's death. The suit could pave the way for future lawsuits across the country for how hospitals react to a variety of emergencies, from viral pandemics to street riots, says a project manager with Aon Corp., a risk-management and insurance advisory firm to hospitals. Lawyers representing the family say the hospital failed to adequately plan for the impending hurricane and are asking for $11.7 million in damages, according to court documents. Attorneys for the hospital say the event was an unforeseen disaster and beyond anyone's control. The woman was one of 16 patients who died at the hospital during Katrina. The lawsuit could make hospitals across the country liable if their power gets knocked out by snowstorms, tornadoes, or other calamities, says a Tulane University law professor following the case. "I'm not at all sure hospitals in the past had thought about their liability for lack of emergency preparedness," he says. "This changes that."
Source: http://www.usatoday.com/news/health/2010-01-10-katrina-hospital-lawsuit_N.htm

34. *January 10, KJRH 2 Tulsa* – (Oklahoma) **Watermain break at Hillcrest hospital causes damage.** Tulsa, Oklahoma, firefighters and city crews worked to get the break under control at Hillcrest Medical Center Sunday night. Firefighters say a three-inch main broke, flooding the records room at the hospital. No one was hurt and no patients were affected. People at the hospital did still have water, but firefighters had to turn off

the sprinkler system to repair the line. Since the sprinkler system was shut down, firefighters stayed at the hospital to monitor things in case a fire did happen. Once the water drains, the hospital will be able to pump it out.
Source: http://www.kjrh.com/news/local/story/Watermain-break-at-Hillcrest-hospital-causes/_6w9ZzC_WUy88VX5p1oNIQ.cspx

35. *January 8, KPCC 89.3 Pasadena* – (California) **Former UCLA medical researcher pleads guilty to illegally accessing patients' medical records.** A former UCLA Healthcare System employee pleaded guilty Friday to four counts of illegally reading private and confidential medical records, the U.S. Attorney's Office announced. Appearing before a United States Magistrate judge, the man admitted to obtaining identifiable health information. He is one of the first people in the nation to be convicted of violating the privacy provisions of HIPAA, the agency reported. While employed in October 2003 with the UCLA School of Medicine he received a dismissal notice based on poor job performance. Following the incident he continued a weeks-long illegal accessing of patient records and those of various celebrities, prosecutors said. According to court documents, he accessed the records system 323 times during the three-week period.
Source: http://www.scpr.org/news/2010/01/08/zhou/

[Return to top]

Government Facilities Sector

36. *January 10, Associated Press* – (National) **Budget cuts force tough choices on court security.** On many days, the metal detectors sit silent at the busiest courthouse in Maine. People arriving for everything from child custody hearings to murder trials walk through the machines without a beep. The detectors are off because the court can not pay for officers to run them. With the recession prompting steep cuts to state and local budgets, courts around the country are facing the tough decision of whether to reduce court services or cut back on security. For many, it is a disturbing choice in a post-9/11 world. When cuts are made to security staff, it compromises the safety of the courthouse, said a security expert for the National Center for State Courts. ''People feel that court security is one area that should receive special consideration for funding since it involves protecting the general public who comes to courthouses for services,'' he said. But some courts have already reduced security staff, others might have to consider it if budget problems do not get better soon. A few just are not filling long-held vacancies. To help save money, many courthouses have closed one day a month, furloughed employees and temporarily delayed jury trials. The cutbacks in state courts come as threats to federal judges and prosecutors have jumped dramatically. The government report issued last week found such threats more than doubled in the past six years, growing from 592 in 2003 to 1,278 in 2008.
Source: http://www.nytimes.com/aponline/2010/01/10/us/AP-US-Courthouse-Security-Cuts.html?_r=1

37. *January 8, Homeland Security Newswire* – (National) **The Pentagon's cybersecurity worries.** At the Pentagon, they are not that concerned about a full-scale attack on the military's networks — even though the modern American way of war depends so heavily on the free flow of data; in the military, there is now broad agreement that one cyber threat trumps all others: electronic espionage, the infiltration (and possible corruption) of Defense Department networks. Well-placed spy software not only opens a window for an adversary to look into American military operations. This window can also be used to extract information — everything from drone video feeds to ammunition requests to intelligence reports. Such an opening also gives that enemy a chance to introduce his own false data, turning American command-and-control systems against themselves.
Source: http://homelandsecuritynewswire.com/pentagon-s-cybersecurity-worries

[Return to top]

Emergency Services Sector

38. *January 11, North Andover Eagle Tribune* – (Massachusetts) **Officer's stolen gun found in Lawrence.** A stolen handgun belonging to a Burlington, Massachusetts, police officer was recovered after it was illegally fired within earshot of the police station by an admitted heroin dealer early Sunday, police said. The 18 year old, of Lawrence, was arrested and charged with firing the stolen Glock, which police believe he did to impress some girls. The suspect said he purchased the gun "from a guy in Haverhill," police said. The unidentified Burlington police officer reported the Glock stolen from his car in November, Lawrence's police chief said.
Source: http://www.eagletribune.com/punews/local_story_011040424.html

39. *January 11, Firehouse.com* – (New York) **Blaze at N.Y. fire station ruins apparatus, offices.** Fire gutted the fire station in Ashland, New York destroying the town's apparatus, ambulance, and the town hall, according to WTEN, News 10, the local television station for the area. The fire started on Sunday morning and crippled Ashland's fire department and ruined its offices. The station had four fire trucks and a brand new ambulance all destroyed. Town's municipal offices were also gutted. The damage is worth more than half a million dollars, a conservative estimate.
Source: http://www.firehouse.com/topics/news/blaze-ny-fire-station-destroys-apparatus-town-offices

40. *January 8, Washington Examiner* – (District of Columbia) **Police probe D.C. officer's claim that gun was stolen in carjacking.** Authorities are searching for a D.C. police lieutenant's service weapon that went missing after a carjacking in Prince George's County, multiple police sources said. The veteran police officer told investigators that his weapon was stolen while his vehicle was stopped late last Wednesday near Temple Hills, law enforcement sources told The Examiner. Police used K-9 units Wednesday night and Thursday to try sniff out the missing gun. A teenage boy has been taken into custody in the case, police said. The teenager denied stealing the gun and said he knew the officer personally, said police sources familiar with the ongoing investigation. The

loss of his gun could be a problem for the officer because this is the third time he has lost his service weapon, according to two sources within the Metropolitan Police Department. Police officers are responsible for their service weapons and can be terminated for losing them through improper safekeeping or making poor personal choices.
Source: http://www.washingtonexaminer.com/local/Authorities-probe-officers-claim-that-service-weapon-was-stolen-80997787.html

41. *January 8, ComputerWorld* – (National) **White House calls for IT boost to fight terrorism.** The White House report on the failed bombing attempt of a U.S airliner on Christmas Day highlights the challenges U.S intelligence agencies face in correlating terrorism-related information gathered from multiple databases and sources. The review, released on January 7, identified an overall failure by intelligence agencies to "connect the dots," despite having enough information at their disposal to have potentially disrupted the botched attack. The problem, according to the report, was not a lack of information sharing between government agencies but a failure by the intelligence community to "identity, correlate and fuse into a coherent story all of the discrete pieces of intelligence held by the U.S. government." In listing the various causes for this failure, the report noted that information technology within the counter-terrorism community "did not sufficiently enable the correlation of data that would have enabled analysts to highlight the relevant threat information."
Source: http://www.computerworld.com/s/article/9143517/White_House_calls_for_IT_boost_to_fight_terrorism

[Return to top]

Information Technology Sector

42. *January 11, SC Magazine* – (International) **Pakistani cyber crime website hit by hacker who is able to access database.** Details of a political website being hacked has been reported when a sensitive site was hit by a hacker who managed to gain access to the email database. After two political websites were hit last week, the Pakistani National Response Center for Cyber Crimes, part of the Federal Investigation Authority, was also hit last week. A senior security adviser at Trend Micro said that the hacker 'zombie_ksa' states on the defaced page: 'your whole database and emails are leaked â ¦. I was really excited to read, see what the f__k is private in here lOl'. The hacker then boasted in a forum posting about the hit, saying: "I was browsing Propakistani.pk, so I saw [a] post about how to register [a] complaint with [the] FIA cyber crime. So I feel to check [their] security, and I started [a] penetration test on their web server, unfortunately I got access! And they got Pwned! That sounds crazy! I got [the] whole database! And email backup! Everything!" The adviser said that zombie_ksa posted two screen shots, one of the hacked site and a second one demonstrating his access to their email database.
Source: http://www.scmagazineuk.com/pakistani-cyber-crime-website-hit-by-hacker-who-is-able-to-access-database/article/160969/

43. *January 11, ComputerWorld* – (International) **Microsoft will patch Mac Word to comply with court order.** Microsoft will patch Word on the Mac to comply with a federal court's ruling requiring it to remove custom XML technology from its popular word processing software, the company confirmed last week. On January 9, Microsoft issued an update for Word 2003 for Windows to abide by the same ruling. In late December, a federal appeals court affirmed a lower court's injunction that barred Microsoft from selling Word 2007 and Word 2003 starting Monday, January 11 unless it dumped custom XML features from the software. In May 2009, a Texas court also ordered Microsoft to pay developer i4i nearly $300 million in damages, court costs and interest for allegedly violating the Canadian company's custom XML patent. According to a Microsoft spokesman, Word 2003, which was also named in the injunction, must be modified because customers purchasing or licensing Word 2007 have "downgrade" rights to the older edition. Microsoft posted an update for Word 2003 for Windows on its download center on January 9.
Source: http://www.computerworld.com/s/article/9143658/Microsoft_will_patch_Mac_Word_to_comply_with_court_order

44. *January 10, United Press International* – (International) **Philippine government web sites hacked.** Hackers in the Philippines have defaced a government Web site, the fifth such attack on such sites in a month, officials said. Hackers left a message on the government's Technical Education and Skills Development Authority site mocking the country's upcoming automated elections, GMANews.tv reported on January 10. "What is going to be used in the elections? Blade server? Juniper firewall?" the message read. The hackers had previously victimized the Web sites of the Department of Health, Department of Social Welfare and Development, National Disaster Coordinating Council, and Department of Labor and Employment, GMANews said. Philippine government officials expressed worry over the security of the May automated elections.
Source: http://www.upi.com/Top_News/International/2010/01/10/Philippine-government-Web-sites-hacked/UPI-77471263162325/

45. *January 8, DarkReading* – (International) **Red Condor warns of highly personalized spear-phishing campaign.** Email security experts at Red Condor today issued a warning for an aggressive spear phishing email campaign inviting recipients to "apply a new set of settings" to their mailboxes because of a recent "security upgrade" of their mailing service. An embedded link in the email connects users to a web site that appears to be a Microsoft' Office Outlook' Web Access page, including official Microsoft' and Microsoft Office logos. On the page, users are directed to "download and launch a file with a new set of settings for your e-mail account." The executable is actually a Zbot Trojan virus similar to Trojans distributed in recent H1N1 and Facebook phishing attacks. Initially identified and blocked by Red Condor's Zero Minute Defense System early the morning of January 7, the campaign has still only been detected by a few virus scanners. "This spear phishing campaign is unusual in that it is highly personalized and is targeting a very large number of domains with a customized message for each domain," said the president and CEO of Red Condor. "Spear phishing campaigns usually target a single organization or domain, but this

attack broke the mold as the volume and targets are very high."
Source: http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=222300161&subSection=Application+Security

46. *January 8, SC Magazine* – (International) **Major flaws in USB stick software leads to secure drives being unlocked easily.** Reports claiming that hardware-encrypted USB flash drives were hacked earlier this week have revealed a major flaw in the products' design. German security firm SySS published reports detailing the vulnerabilities in Kingston, SanDisk and Verbatim flash drives, and detailed how they can be hacked. It claimed that the vulnerability lies in a major flaw in the design of the affected products. It said that there was an inherent design error in the software that runs on the host PC to verify the correctness of a user's password, and is not secure. SySS said it was equivalent to a single shared backdoor password for all of these devices, as security analysts were able to write a program that sent the 'unlock' code regardless of the password entered, and gain immediate access to the flash drive's entire contents. SanDisk has issued a security bulletin, saying it had 'recently identified a potential vulnerability in the access control mechanism and has provided a product update to address the issue'. It said that the issue is only applicable to the application running on the host and does not apply to the device hardware or firmware, and all Enterprise USB flash drives being shipped to customers as of today contain the product update.
Source: http://www.scmagazineuk.com/major-flaws-in-usb-stick-software-leads-to-secure-drives-being-unlocked-easily/article/160898/

47. *January 8, PC World* – (International) **Hacking takes lead as top cause of data breaches.** Hacking has topped human error as the top cause of reported data breaches for the first time since such tracking began in 2007, according to the Identity Theft Resource Center's 2009 Breach Report. In its report, titled "Data Breaches: The Insanity Continues," the non-profit ITRC found that 19.5 percent of reported breaches were due to hacking, with insider theft as the second most common cause at 16.9 percent. For the past two years, "data on the move," a typically human-error loss of a portable devices such as laptops or even briefcases, was the most common reported cause. The ITRC is careful to note that its statistics are based on incomplete data, as differing laws and practices among different states mean that some breaches are not reported publicly, and the cause of the breach is not listed for about one third of those that are reported. But according to the data available, the number of reported data breaches dropped since 2008, but was still more than in 2007. Last year, there were 498 breaches recorded by the ITRC, with 657 in 2008 and 446 in 2007.
Source: http://www.networkworld.com/news/2010/010810-hacking-takes-lead-as-top.html?hpg1=bn

48. *January 8, V3.co.uk* – (International) **Microsoft set for small Patch Tuesday.** IT administrators will be relieved to hear that next week's Microsoft Patch Tuesday will see just one bulletin addressing a single vulnerability in Windows. A Microsoft security spokesman announced the news in a blog posting on January 7, explaining that the single vulnerability is rated as 'critical' on Windows 2000 and 'low' for all other platforms. "Customers with Windows 2000 systems will want to review and deploy this

update as soon as possible but, as we will show in our release guidance next week, the Exploitability Index rating for this issue will not be high, which lowers the overall risk," he wrote. The news will come as something of a relief to IT staff, who have recently had to cope with mammoth security updates from Microsoft. In October, the firm released 13 bulletins addressing a whopping 34 vulnerabilities. But there was also cause for concern among security professionals, as the spokeman pointed out that Microsoft's security team is not addressing a known flaw in its Server Message Block protocol which could enable denial-of-service attacks.
Source: http://www.v3.co.uk/v3/news/2255836/microsoft-set-fix-patch-tuesday

49. *January 8, The Register* – (International) **Fix finalized for SSL protocol hole.** Engineers have signed off on a fix for a potentially serious vulnerability in the SSL, or secure sockets layer, protocol that secures email, web transactions and other types of sensitive internet traffic. The final draft updates the industry-wide specifications for SSL, which is also referred to as TLS, or transport layer security. Now that the Internet Engineering Task Force has approved it for publishing as a formal standard, it will update RFC 5246, the most recent request for comments that maps out the current SSL protocol. The new protocol overhauls the way SSL-enabled software renegotiates encrypted sessions so it is no longer possible for attackers to inject malicious payloads into encrypted traffic passing between two endpoints. The vulnerability violated one of the core guarantees provided by SSL by making it possible to perform man-in-the-middle attacks that could steal sensitive data or tamper with secure transactions. Since the flaw was disclosed in November 2009, many software makers have disabled the renegotiation feature in their programs, a tweak that meant their applications were technically not compliant with official specifications laid out in RFCs that govern SSL. The new protocol provides a longer-term fix by restoring renegotiation capabilities without putting SSL sessions at risk.
Source: http://www.theregister.co.uk/2010/01/08/ssl_fix/

50. *December 8, eWeek* – (International) **Oracle preps critical update with 24 security fixes.** Oracle is planning to release an update that includes 24 security patches affecting numerous products, including the Oracle Database and Oracle E-Business Suite. The update addresses 10 security vulnerabilities related to the database, including one in Oracle Secure Backup. Two of the vulnerabilities can be exploited remotely without authentication, Oracle said in a pre-patch advisory. Oracle BEA products are the subject of five security fixes, all of which are remotely exploitable over a network without a user name and password. One of the security holes plugged by the update is a flaw in Oracle JRockit with a CVSS base score of 10.0, the highest score possible. The update plugs three remotely exploitable security holes in Oracle's application server, as well as providing a fix for the PeopleSoft and JD Edwards Suite. The update also has two new security fixes for the Oracle Primavera Products Suite and three for Oracle Application Server.
Source: http://www.eweek.com/c/a/Database/Oracle-Preps-Critical-Update-With-24-Security-Fixes-581367/

For more stories, see items **17**, **53**, and **55**

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

51. *January 11, Data Center Knowledge* – (National) **New data centers: DHS, Peak 10, more.** Last week saw a flurry of news about new data centers being planned, built or finished. General Dynamics Information Technology (GD) said last week that it has opened an enterprise data center in Westminster, Colorado, to support the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS). The new data center, which is certified under the Leadership in Energy and Environmental Design (LEED) standard for energy efficient buildings, will provide centralized, round-the-clock support for USCIS and employ approximately 100 IT workers when fully staffed. Peak 10 Inc., a provider of data center and managed services, announced the addition of a second facility on its Atlanta campus. The completion of the 10,000 square foot facility will bring the company's Atlanta's total footprint to more than 33,000 square feet. This expansion comes on the heels of Peak 10's recent $95 million credit facility expansion led by RBC Capital Markets. Ground will be broken on the state of Massachusetts' new $110 million state data center in Springfield this spring, with the 115,000-square-foot facility scheduled to be up and running in May 2012, according to local media reports. The Cleveland Clinic has purchased 14 acres of land in Brecksville, Ohio and plans to use the site to build an 80,000 square foot data center, Cleveland Business News reported.
Source: http://www.datacenterknowledge.com/archives/2010/01/11/new-data-centers-dhs-peak-10-more/

52. *January 11, Network World* – (International) **Half of all data centers understaffed, Symantec survey finds.** Fifty percent of IT executives say their data centers are understaffed, and companies are still looking for more ways to cut costs, according to Symantec's latest "State of the Data Center" report. Sixteen percent of survey respondents said their data centers are extremely understaffed, and another 34 percent called their data centers somewhat understaffed. At the same time, data centers are becoming more complex and harder to manage, with more applications, data and increasingly demanding service-level agreements. For its third annual data center report, Symantec commissioned Applied Research to survey data center specialists in 1,780 enterprises worldwide, each with at least 1,000 employees. The vast majority of companies said they are having trouble finding enough money and enough qualified applicants to keep their data center staff at healthy levels. Nonetheless, 45 percent of companies say their data centers are appropriately staffed, and 5 percent reported being

overstaffed.
Source: http://www.networkworld.com/news/2010/111110-data-centers-understaffed.html?hpg1=bn

53. *January 11, eWeek* – (International) **McAfee: spammers turn to free web hosting services.** Spammers are increasingly turning to free-hosting Web sites to provide spam URLs, according to a new report from McAfee. In its "January 2010 Spam Report", McAfee notes the trend is turning into an "all-out gold rush" as dozens of these free-hosting sites have sprung up to provide Web space for anyone who requests it. According to the report, all of the sites most heavily abused by spammers seem to be related to 0catch.com, which serves up a number of free-hosting sites to anonymous users. These types of services are good for spammers because such sites may have been around for awhile and have legitimate traffic associated with them, the report explained. That edge could give spammers a few hours worth of an edge against anti-spam vendors before they can blacklist the host, the report warns. Just what should be done about these services is a difficult question, opined the anti-spam technology lead for McAfee labs and co-author of the report. The researcher said he would like to see more security technologies brought to bear within free hosting sites to fight spam and viruses. Spam volumes shot up December 14 after trending downward for more than a month, according to the McAfee report, with much of that boost coming in the form of Chinese pharmacy spam. The resurgence of spam from China came at a time when the country tightened its domain registration process, which some researchers predicted will actually help combat malicious activity.
Source: http://www.eweek.com/c/a/Security/McAfee-Spammers-Turn-to-Free-Web-Hosting-Services-371651/

54. *January 8, IDG News Service* – (National) **FCC warns of impending wireless spectrum shortage.** The U.S. Federal Communications Commission chairman said an impending shortage of wireless spectrum in the U.S. will dampen future economic growth unless action is taken to fix the problem. "Our data shows there's a looming crisis, not tomorrow, not next week, not next year, but at some point in the future," the chairman told attendees at the International Consumer Electronics Show (CES) in Las Vegas on on January 8. "The record is pretty clear that we need to find more spectrum," he said. The FCC has identified the limited supply of wireless spectrum as one of the factors that could limit the growth of broadband Internet services in the U.S., which could result in slower economic growth and job creation. Wireless spectrum will be addressed, along with other factors affecting broadband access and services, in a national broadband plan that the FCC is now assembling. The plan was originally due to be completed next month, but the FCC received a 30-day extension from the U.S. Congress. Given the urgency of the problem, the FCC will have to move quickly to avoid demand for wireless broadband outstripping the supply of available spectrum, the chairman said, adding that other measures are needed to ensure that wireless networks are used as efficiently as possible.
Source:
http://www.computerworld.com/s/article/9143579/FCC_warns_of_impending_wireless_spectrum_shortage

55. *January 8, The Register* – (International) **Brit ISP knocked offline by Latvian DDOS.** About 30,000 customers of the Cheshire-based ISP Vispa were forced offline for almost 12 hours today by a DDOS attack traced to the Baltic state of Latvia. Broadband service has now been restored, a spokesman said, but customers are unable to call customer service because the firm's phone system was also crippled by the attack. "As a result of a major denial of service attack on our network we suffered a severe outage between 1am and 12.30pm Friday January 8," Vispa's commercial director said. "All services have now been restored except for our phone system which has been affected as part of the problem. We are currently working with suppliers to have the main numbers diverted to other lines within the office but expect to restore the system by the end of today." DDOS attacks on British ISPs apparently from inside former Soviet bloc countries are common, but it is rare for them to have such a paralyzing effect.
Source: http://www.theregister.co.uk/2010/01/08/vispa_ddoa/

[Return to top]

Commercial Facilities Sector

56. *January 10, Associated Press* – (California) **N. California rocked by quake.** A powerful offshore earthquake rattled communities in far northern California, cutting power to thousands of customers, causing minor damage to homes and businesses, and forcing many people to seek treatment for cuts and bruises from falling debris. The 6.5 magnitude temblor hit at about 4:27 p.m. Saturday and was centered in the Pacific Ocean about 22 miles west of Ferndale. Dozens of people suffered minor injuries. In Eureka, north of Ferndale, residents of an apartment building were evacuated, and an office building and two other commercial structures in the town of about 26,000 people were declared unsafe for occupancy, according to a Humboldt County spokesman. Several people received minor cuts and scrapes from broken glass at the Bayshore Mall in Eureka, and an elderly person fell and broke a hip, authorities said.
Source: http://www.caycompass.com/cgi-bin/CFPnews.cgi?ID=10388551
See items **4** and **59**

57. *January 10, Reuters* – (International) **Armed attack highlights athletes' vulnerability.** A second armed attack in the space of a year on a bus carrying a national sports team has highlighted the vulnerability of top-level athletes and the publicity such ambushes attract. Two members of Togo's soccer delegation died when gunmen attacked the team bus on Friday as it traveled to the African Nations Cup in Angola. The Angola attack, which has resulted in the Togo captain announcing on Sunday his players will return home, has focused unwelcome attention on the soccer World Cup in five months' time. South Africa, which has already successfully staged rugby and cricket World Cups, will be the first African nation to host the world's second biggest sports festival after the Olympic Games. On Saturday, the chief World Cup organizer dismissed any comparison with the Nations Cup at the start of a momentous year for African soccer. However, the international security director of the Asia-Pacific Foundation, a London-based think tank, said many people had been looking to the

Angola tournament as a litmus test for the World Cup. He said the magnitude of the soccer World Cup made it an attractive target for militants seeking maximum publicity. Security is going to be a major problem at the New Dehli Commonwealth Games in October following the militant attacks in Mumbai in 2008. "Even a smaller attack up to a month before the Games will create problems for the authorities because there will be panic, countries like Australia and England will start panicking whether they can send their teams," said the expert.
Source: http://www.reuters.com/article/idUSTRE60915H20100110

58. *January 10, WJFW 12 Milwaukee* – (Wisconsin) **Police looking for man who threw Molotov cocktail.** Milwaukee police are looking for a suspect who threw a molotov cocktail, otherwise known as a flaming gasoline bomb, at a gas station cashier last month. Video from the store's security camera shows a masked man walking into the store with a flaming bottle on December 29. He throws the bottle at the cashier, narrowly missing a customer, as it burst into flames. The cashier, who was protected by bulletproof glass, was not hurt. Police say the incident came only days after a suspect in a 2007 robbery at the same store was arrested, so they believe there may be a connection. Police have made no arrests in this case.
Source: http://www.wjfw.com/stories.html?sku=20100110212259

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

59. *January 9, Bay City News Service* – (California) **Utility crews say earthquakes didn't appear to damage Calaveras Dam.** Utilities crews say two recent earthquakes have not caused any detectable damage to the Calaveras Dam, a 75-year-old structure holding back a reservoir that straddles Santa Clara and Alameda counties. A 4.1-magnitude earthquake Thursday and a 3.7-magnitude quake Friday were both centered along the Calaveras Fault near the Calaveras Reservoir, according to the U.S. Geological Survey. The San Francisco Public Utilities Commission dispatched workers and found no signs of damage to the reservoir infrastructure, including Calaveras Dam, an earth-filled structure built in 1925. Water in the reservoir is currently lowered by 60 percent of full capacity due to concerns about the seismic stability of the dam.
Source: http://www.contracostatimes.com/news/ci_14157183
See items **4** and **59**

60. *January 8, Idaho Statesman* – (Idaho) **Army Corps considers long term repairs at Lucky Peak Dam.** The U.S. Army Corps of Engineers plans to place a seismograph on the Lucky Peak Dam in Idaho and conduct emergency exercises to minimize the risks

of the dam. And the agency plans further studies for repairs and modifications to the dam to bring it up to industry standards, the corps said Thursday. The interim risk study did not indicate a need for changes to water management operations at the dam. "There's no evidence an emergency situation exists or is about to occur, but we've identified dam safety issues that don't meet dam industry standards," the corps project manager said. In 2007, the corps announced a new, risk-informed process to optimize public safety and to prioritize dam safety deficiencies at its 600-plus dams nationwide. The Lucky Peak review was a part of that process.
Source: http://www.idahostatesman.com/outdoors/story/1034559.html

61. *January 8, Times-Georgian* – (Georgia) **FEMA says it might not pay for repairs to Twin Lakes dam.** Reports from the Federal Emergency Management Agency (FEMA) suggest the agency might not fund the necessary repairs to the Twin Lakes Dam near Villa Rica, Georgia, which was damaged in the September floods. Should FEMA not fund the repairs, it would force the county to either pay for the $1 million reconstruction project or drain one of the lakes permanently. The dam, which is actually Twin Lakes Road that runs on the far side of the smaller of the two lakes, suffered significant damage when flood waters from storms on September 20 and 21 completely washed out the spillway and ripped a portion of the road from its embankment, rendering the dam unstable. Since then, crews have nearly completely drained the lake but recent rains have since filled it almost completely. A pump has been set up to keep the level down, but its impact is minimal. The public works superintendent for the county, said the problem with the dam largely stems from the fact that when the road was modified from its original use as a railway, silt from the lake was used to widen the roadway and provide a base for the road itself. That silt washed away in the flooding, he said, and in order to secure the dam, much of the remaining silt that the road rests upon would need to be exchanged for clay and other more resolute materials. FEMA's insistence on exclusively repairing the road without addressing the core of the dam itself would be insufficient, he said, and there is no way to secure the lake without doing due diligence on the dam as well as the roadway.
Source: http://www.times-georgian.com/pages/full_story/push?article-FEMA+says+it+might+not+pay+for+repairs+to+Twin+Lakes+dam &id=5510029&instance=home_news_top

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Web site: http://www.dhs.gov/iaipdailyreport

Contact Information

Content and Suggestions:	Send mail to 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 nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer