Homeland Security

Daily Open Source Infrastructure Report for 22 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 Dayton, Ohio officials have ordered about 50 employees to evacuate the Lord Corporation APD aerospace plant near where a truck leaking hazardous acids forced the shutdown of Interstate 75 and created a green cloud drifting westward. (See item **13**)
- According to the Associated Press, federal authorities are investigating a rash of church fires in East Texas, where seven such blazes have been reported since January 1. (See item **58**)

Fast Jump Menu

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 21, Pensacola News Journal* – (Florida) **Vandals damage Gulf Power equipment.** Vandals shot vital equipment at a Gulf Power Company substation in Milton, causing a power interruption to 4,400 customers. “It appears to us that this equipment, what we call an interrupter, was shot,” a Gulf Power public affairs manager said in a news release. “The only way to repair it safely was to turn the entire substation

off." Gulf Power customers in a general area bordered on the west by the Blackwater River, on the north by Interstate 10, and on the south by Nichols Lake Road temporarily lost power service.
Source:
http://www.pnj.com/article/20100121/NEWS01/1210321/1006/NEWS01/Vandals-damage-Gulf-Power-equipment

2. *January 20, U.S. Environmental Protection Agency* – (California) **Southern California pipeline firm to pay $1.3 million to resolve Pyramid Lake oil discharges.** Pacific Pipeline Systems LLP, a Long Beach, Calif.-based oil transport company, has agreed to pay a $1.3 million civil penalty and discontinue the use of a section of pipeline through an unstable section of mountains to resolve a Clean Water Act violation, the Justice Department and U.S. Environmental Protection Agency (EPA) announced on January 20. The agreement resolves a complaint filed in federal court in Los Angeles for the discharge of crude oil into Pyramid Lake, located about 60 miles northwest of downtown Los Angeles. In March 2005, a landslide caused a portion of Pacific Pipeline Systems' Line 63, an underground pipeline that runs from Bakersfield, California to Los Angeles, to fail. The resulting pipeline break discharged approximately 3,393 barrels of oil, much of which flowed into Pyramid Lake, which is part of the California Aqueduct and is a potential drinking water supply. As part of the agreement, Pacific Pipeline Systems will discontinue use of approximately 70 miles of the Line 63 pipeline that travels through the Tehachapi Mountains, portions of which are geologically unstable. The agreement does allow for the reuse of the pipeline. Prior to that, Pacific Pipeline must perform specific actions to relocate the pipeline into more geologically stable areas or improve its resistance to earth movement.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/3894206BA9BE63FB852576B10076B3C8

3. *January 20, KFDM 6 Beaumont* – (Texas) **Fuel gas leak at Total keeps some contract workers home.** The Total Refinery in Port Arthur is investigating a fuel gas leak on January 20 that prompted the plant to send some contract workers home for the day, according to information provided to KFDM News by a Total spokeswoman. She said there is no danger to the public or employees. "We have a fuel gas leak that we're trying to isolate," she told KFDM News. "It's our practice to keep extra people out of the refinery while we respond to such issues." The plant is operating normally, according to her, and all Total employees are on the job. She said an unspecified number of contract workers were sent home or told not to report Wednesday because they're not needed at the time. Total workers are conducting fence line monitoring and have not detected any unsafe levels of vapors, according to her.
Source: http://www.kfdm.com/news/total-36259-workers-avery.html

For another story, see item **5**

[Return to top]

Chemical Industry Sector

4. *January 21, Dayton Daily News* – (Ohio) **I-75 lane closures caused by acid leak expected through morning.** It could be mid-morning Thursday, January 21, before all lanes of Interstate 75 north reopen because of the chemical spill from a semi-trailer January 20 night that led to an hours-long shut down of the north and south lanes, an official said. At 8:53 p.m., January 20, authorities were trying to reopen one northbound lane within the hour, said a coordinator of the Dayton Regional Hazardous Materials Unit. He explained that 100 to 300 gallons of run-off from waste material aboard the semi-trailer would have to be sopped up and the vehicle would have to be towed from the interstate before that could happen. He said hazmat workers traced the leak to a 300-gallon container of sulfuric acid, but they were still not clear how the leak began. The Ohio Highway Patrol and the Public Utilities Commission of Ohio will be investigating, he said. According to a preliminary investigation, the semi-trailer loaded with hydrochloric, sulfuric and phosphoric acids left West Carrollton from Veolia ES Technical Solutions on the afternoon of January 20 enroute to Michigan when it was pulled over by a trooper around 5:15 p.m.
   Source: http://www.daytondailynews.com/news/dayton-news/i-75i-75-lane-closures-caused-by-acid-leak-expected-through-morning-502728.html?imw=Y
   See item **13**

5. *January 20, Reuters* – (Louisiana) **Exxon reports Baton Rouge incident.** Exxon Mobil Corp on January 20 reported an unspecified "incident" that occurred Tuesday afternoon at its 503,000 barrels-per-day Baton Rouge, Louisiana, oil refinery's sulfur plant. "At about 1 p.m. Tuesday, the ExxonMobil Baton Rouge Refinery responded to an incident at our sulfur plant located south of Gulf States Road," an Exxon spokesman added in an email. Some on-site personnel were asked to shelter-in-place as a precaution, he said, adding there were no reported injuries nor off site impacts. "Per normal procedure, ExxonMobil notified all appropriate agencies," he said. He said he had no information about the refinery status, citing company policy of not commenting on day-to-day operations.
   Source: http://www.reuters.com/article/idUSN2015457920100120?type=marketsNews

For more stories, see items **28** and **30**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *January 21, San Diego Union-Tribune* – (California) **Problems at nuclear plant concern regulators.** Nuclear regulators are concerned that operators at the San Onofre nuclear power plant botched a series of calls last week, resulting in the simultaneous shutdown of two safety backup systems and placing operators on standby to shut down a nuclear reactor. The situation was not considered dangerous, because the systems in question come into play only in an emergency. Plant workers were able to bring up one of the backup systems after 15 minutes, forestalling a reactor shutdown. However, Nuclear Regulatory Commission (NRC) spokesman said the fumble exemplifies continuing safety problems at San Onofre that regulators want fixed. "This raises

further concerns for us because it's another example of a human performance failure caused by miscommunication," the spokesman said. The NRC recently assigned a third inspector to monitor plant operations, saying plant officials weren't making sufficient progress in improving San Onofre's safety culture. The NRC has cited the plant for safety violations over the past four years, and many of those lapses are blamed on human error.
Source: http://www.signonsandiego.com/news/2010/jan/21/problems-nuclear-plant-concern-regulators/

7. *January 21, Associated Press* – (Kentucky) **Ky. Senate passes bill to allow nuclear plants.** Legislation to lift Kentucky's ban on the construction of nuclear power plants steamed through the Senate on Wednesday but could get unplugged in the House. The bill, which cleared the Senate on a 27-10 vote, is backed by the governor but the house speaker said he does not think the measure will pass the House. State law currently prohibits a nuclear power plant from being built in Kentucky until there is a permanent storage facility to contain the nuclear waste. A proposed high-level radioactive waste facility at Yucca Mountain in Nevada has been discussed for years. An Independent senator from Paducah said Wednesday his bill would put Kentucky on "equal footing" with other states if the federal government ever approves new nuclear plants.
Source: http://abcnews.go.com/Business/wireStory?id=9621977

8. *January 20, Red Wing Republican Eagle* – (Minnesota) **On-site brigade extinguishes fire at nuclear plant.** Fire broke out Wednesday in a non-emergency, non-safeguard diesel generator at Prairie Island nuclear plant. The fire started at 1:17 p.m. during routine testing. The plant's on-site fire brigade responded and extinguished the fire at 1:37 p.m. before the Red Wing Fire Department arrived, according to Xcel Energy, which owns and operates the plant. At 2:55 p.m., the fire reflashed and again was extinguished. Red Wing firefighters were on the scene. There were no injuries, Xcel Energy reported. The fire did not affect Unit 1 or Unit 2 and in no way would have hampered the safe shutdown of operations had that been necessary, officials said. An investigation to determine the source of the fire is under way. Plant personnel notified state, local and tribal government and emergency services agencies, as well as Nuclear Regulatory Commission personnel.
Source: http://www.republican-eagle.com/event/article/id/64144/

9. *January 20, U.S. Nuclear Regulatory Commission* – (Michigan) **NRC proposed $3,500 fine against Michigan-based Engineering Services Inc.** The Nuclear Regulatory Commission has proposed a $3,500 fine against Engineering Services Inc., located in Livonia, Michigan, for repeated failure to properly secure a moisture density gauge containing shielded radioactive sources. NRC conducted an inspection in October 2009 to evaluate the status of improvements the company had committed to make in response to the April 2009 violation associated with the failure to provide two physical barriers to secure a portable nuclear gauge. The company was using only one security barrier. The company's corrective actions consisted of making sure the gauge was properly secured. No fines were levied on the company for the initial violation in April 2009 due to the company's good performance in the previous year and actions

taken to correct the problem. After the follow-up inspection, the NRC staff determined that the company again failed to provide two physical barriers to prevent unauthorized access to the gauge. The NRC proposed a civil penalty of $3,500 because it was a repeat violation of NRC requirements.
Source: http://www.nrc.gov/reading-rm/doc-collections/news/2010/10-001.iii.html

[Return to top]

Critical Manufacturing Sector

10. *January 21, Seattle Post Intelligencer* – (National) **Boeing 747-8 could be vulnerable to hackers.** The Boeing 747-8 is just a few weeks away from taking off for the first time. Before the plane goes into service, the FAA wants to make certain the plane's computer systems cannot be hacked. The FAA states the Boeing 747-7 "will have novel or unusual design features associated with the architecture and connectivity capabilities of the airplane's computer systems and networks, which may allow access to external computer systems and networks." With passengers being able to access on board internet and in flight entertainment systems, there is a chance someone could cause harm to the aircraft's computer systems. The FAA requested similar precautions for the Boeing 787 as well. Boeing must ensure electronic system security protection for the aircraft control domain and airline information domain from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity. It must also ensure that electronic system security threats from external sources are identified and assessed, and that effective electronic system security protection strategies are implemented to protect the airplane from all adverse impacts on safety, functionality, and continued airworthiness.
Source: http://blog.seattlepi.com/airlinereporter/archives/191691.asp?from=blog_last3

11. *January 21, Fayetteville Observer* – (North Carolina) **Equipment fire damages plant in Clinton.** A piece of equipment used to make steel straps caused a fire Thursday morning at DuBose Strapping Inc. in Clinton. "It's not an unusual occurrence," said a plant spokesman. "It happens from time to time, but this was a little more severe." Less than 10 people were working in the plant at 906 Industrial Drive when the fire started about 2:15 a.m. Some of the plant's electrical and filtration systems were damaged. "We expect to be back up in a couple of days," he said. The plant manufactures steel bands that are used to wrap around shipping pallets. During the process, steel is heated to 1,700 degrees, and oil can accumulate on the machinery. That oil tends to burn off, which can cause a small burst of fire, he said. Flames burst through the roof before the workers put it out, he said, but the building was not badly damaged. He did not have an estimate of the damages. The plant is continuing to operate on a regular schedule, he said.
Source: http://www.fayobserver.com/Articles/2010/01/21/969925

[Return to top]

Defense Industrial Base Sector

12. *January 21, Aviation Week* – (National) **USAF chief downplays JSF testing delay.** A testing delay for the F-35 program will prompt an increase in the per-unit cost of the stealthy single-engine fighter "for a period," says the U.S. Air Force chief of staff. The general says the boost will not, however, be enough to breach requirements under the Nunn-McCurdy reporting law, which triggers a mandatory Pentagon review of alternatives and notification of Congress in cases of a significant cost and schedule overrun. The chief says the delay, which he only described as not lasting "multiple years," was necessary. Government officials have indicated that completing testing could take up to 30 months more than planned; the current time-line is to wrap up testing in 2014. The general said the restructuring was needed to reduce the concurrency of development and production, lengthen the testing period and boost the number of test assets available. It also will result in a "less ambitious" production ramp-up, he says. However, he says that the initial operational capability of the first training unit is still on schedule for this year. The slip will create what the U.S. Air Force chief of staff calls a "nose-to-tail" handoff for the Air Force from the F-16, which is currently in operation. It will eliminate the overlap, or margin, between the drawdown of the legacy fleet and introduction of the stealthy single-engine fighter into the inventory, he said.
    Source:
    http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2010/01/21/01.xml

13. *January 20, Associated Press* – (Ohio) **Some evacuations following Ohio acid spill.** In Dayton, officials have ordered about 50 employees to evacuate an aerospace company's plant near where a truck leaking hazardous acids forced the shutdown of Interstate 75 and created a green cloud drifting westward. A plant manager for Lord Corporation APD says employees were sent home early Wednesday evening. A patrol lieutenant says authorities were alerted Wednesday afternoon that a truck had pulled over and was leaking yellow fluid on the highway just north of Dayton. Authorities who arrived on the scene discovered the truck was carrying hydrochloric and sulfuric acid. The patrol does not know how much acid the truck was carrying or how much of the substance leaked onto the road. The highway will be closed for several hours as a hazardous materials crew cleans up the acid. He says authorities are not evacuating nearby areas, but they are keeping an eye on the scene.
    Source: http://www.wfmj.com/Global/story.asp?S=11855821
    See item **4**

[Return to top]

Banking and Finance Sector

14. *January 21, Computerworld* – (National) **Heartland's $60M breach settlement offer not enough, lawyers say.** Lawyers representing financial institutions in a data breach lawsuit against Heartland Payment Systems Inc are calling a recently proposed $60 million settlement offer from the company as way too meager. In a statement released on January 20, the lawyers said the proposed settlement would only pay banks and

credit unions "pennies on the dollar," while releasing Heartland and other potentially liable parties from further legal action. Princeton, New Jersey-based Heartland announced in January 2009 that unknown intruders had broken into its systems and stolen card data. More than 130 million credit and debit cards were believed to have been compromised in the intrusion, making it the biggest ever involving payment card data. Hundreds of banks were affected by the breach. Many of them later sued the payment processor seeking to recover card-reissuance and fraud-related costs. Earlier in January, Heartland and Visa announced a settlement under which Heartland said it would pay up to $60 million to compensate card issuers for breach-related costs. The proposed settlement requires card issuers to release Heartland and Visa from any additional liability. Banks and credit unions affected by the breach have until January 29th to decide if they want to accept the terms of the settlement or not. The proposed settlement will go into effect if at least 80 percent of affected Visa card issuers agree to it.
Source:
http://www.computerworld.com/s/article/9146758/Heartland_s_60M_breach_settlement_offer_not_enough_lawyers_say

15. *January 21, V3.co.uk* – (International) **Security fears dog online banking.** Online banking customers are worried about their financial security, but banks are lagging behind, according to a global survey of 4,500 internet users. The survey identified security as a concern for 86 per cent of online banking users, compared with just 68 per cent for users of government web sites and 64 per cent for online health care. Four out of five wanted better protection than a simple password. "Consumers are very much aware of the threats," the senior manager of identity protection and verification at RSA, told V3.co.uk. "They are not satisfied with simple password protection. Consumers really want and need this security." The manager explained that, while some European banks use two-factor authentication, many UK and US banks are turning to risk-based authentication. A risk-based approach monitors user behavior and applies computer algorithms to usage patterns to determine whether an account has been compromised. Such systems avoid the 'man in the middle' attacks that can defeat two-factor authentication. However, internet users are getting savvier about the threats from phishing and malware. In a similar survey in 2007, 63 per cent of respondents were aware of Trojans, but this had risen to 81 per cent last year.
Source: http://www.v3.co.uk/v3/news/2256508/security-fears-dog-online

16. *January 20, IDG News Service* – (National) **Heartland moves to encrypted payment system.** Responding to its widely reported and massive data breach that took place a year ago, Heartland Payment Systems will be moving to an end-to-end encryption system for payment transactions, according to the Chairman and CEO. "End-to-end encryption is a good way to mitigate the risk of having the kind of compromise that we and hundreds of other companies have had," the CEO said in an interview. "We're using encryption on the front end to keep card numbers out of our merchants' systems, and to also have all the card numbers coming through our network be encrypted throughout, except at the point of decryption," he said. The company, which handles more than 4 billion transactions annually for more than 250,000 merchants, will be

using Thales nShield Connect hardware security module along with Voltage Security's SecureData encryption software as the basis of this capability.
Source:
http://www.pcworld.com/businesscenter/article/187260/heartland_moves_to_encrypted_payment_system.html

17. *January 20, Wall Street Journal* – (National) **U.S. looks to keep bank fee from disrupting markets.** The Treasury Department is consulting with Congress and market participants on the details of the government's planned "financial crisis responsibility fee," a Treasury spokesman said, amid worries that the levy could disrupt the Treasury market. A disruption in the Treasury market would hurt the broader economy by raising interest rates and also would hit the government's own bottom line by boosting the costs of its borrowing at a time when Treasury has to sell massive amounts of debt to cover a trillion-dollar-plus deficit. The Treasury Department spokesman said the Treasury has been tuned in from the beginning on how the fee could affect markets and is broadly considering the concerns of market participants and mulling over a number of technical ideas that have been suggested. Around the time the U.S. President unveils his fiscal 2011 budget, on February 1, the Treasury is expecting to have more details on what form the fee could take, the spokesperson said. To keep the levy from disrupting markets, Treasury could exempt the securities repurchase market for government debt from the 0.15-percentage-point fee, which will be levied on liabilities that are not covered by the FDIC. The roughly $5 trillion repo market is the core of debt markets, where investors and financial firms raise short-term funding secured by government debt securities.
Source:
http://online.wsj.com/article/SB10001424052748704320104575015314043161970.html?mod=googlenews_wsj

18. *January 20, NewsFactor Network* – (International) **DIY cybercrime kits power growth in phishing attacks.** Do-it-yourself (DIY) cybercrime kits are driving a surge in Internet-borne computer infections. DIY kits have been a staple in the cyberunderground for some time. But now they have dropped in price and become more user-friendly. "If you know how to download music or a movie you have the necessary experience to begin using one of these kits," says a senior researcher at security Relevant Products/Services firm Damballa. Indeed, new cybercrooks and veterans alike are using DIY kits to carry out phishing campaigns at an accelerated rate, security researchers say. They have been blasting out fake e-mail messages crafted to look like official notices from UPS, FedEx, or the IRS; or account updates from Vonage, Facebook, or Microsoft Relevant Products/Services Outlook; or medical alerts about the H1N1 flu virus. The faked messages invariably ask the recipient to click on a Web link; doing so infects the PC with a banking Trojan, a malicious program designed to steal financial account logons. Often, the PC also gets turned into a "bot": The attacker silently takes control and uses it to send out more phishing e-mail. Generally sold for $400 to $700, the kits come with everything an individual needs to begin infecting PCs. Selling software is legal; what a user does with it can get the user into trouble.

Source: http://www.newsfactor.com/news/DIY-Cybercrime-Kits-Spur-Phishing/story.xhtml?story_id=110003LAJ3EU

19. *January 20, Reuters* – (National) **US FDIC geared up for busy year of bank failures.** The U.S. agency charged with dismantling or selling off failed banks said it is equipped to deal with what it sees as a busy 2010, according to remarks to be delivered before Congress on January 21. The Federal Deposit Insurance Corp expects that bank failures will remain elevated this year, said the director of the FDIC's division of resolutions and receiverships. Regulators seized 140 banks in 2009, the highest annual level since 1992 in the wake of the savings and loan crisis. Many of the institutions collapsed due to deteriorating loans from the credit boom. "While the economy is showing signs of improvement, recovery in the banking industry tends to lag behind other sectors. We expect to see the level of failures continue to be high during 2010," the director said in testimony posted to the website of the House of Representatives subcommittee on financial institutions. The FDIC has said it expects the total bill for bank failures to reach $100 billion for the period of 2009 through 2013. The woes in the banking industry have migrated from home mortgages to commercial real estate (CRE), especially for community banks that tend to have higher concentrations of commercial loans.
Source: http://www.reuters.com/article/idUSN2017182020100120

20. *January 20, Associated Press* – (California) **SoCal businessman convicted of $62M Ponzi scheme.** A Huntington Park businessman has been convicted of federal charges for running a $62-million investment scheme that bilked more than 2,000 people. The U.S. attorney's office says the defendant was convicted on January 19 of mail fraud and making false statements. He could face up to 125 years in federal prison. He remained jailed on January 20 without bail. Prosecutors say the defendant's company, Best Diamond Funding, promised high returns on real estate investments to mainly blue-collar clients — some of whom mortgaged their homes or emptied their retirement savings. Prosecutors say he used about $30 million from later investors to pay earlier ones and invested little of the money. The scheme was advertised in Spanish-language magazines, on the Internet, and in seminars.
Source: http://www.mercurynews.com/breaking-news/ci_14231746

[Return to top]

Transportation Sector

21. *January 21, Charleston Daily Mail* – (West Virginia) **Runway damage assessed at Yeager.** A day after a failed takeoff at Yeager Airport left significant damage to a strip of impact-absorbing soft concrete at the end of the runway, officials were at work assessing the damage and readying for repairs. Airport officials are now scrambling to replace the Engineered Material Arresting System (EMAS), which they said saved the lives of 31 passengers and three crew members Tuesday afternoon. EMAS has the consistency of ash and is installed in segments that are coated in soft concrete. The material is designed to collapse under the weight of an aircraft, bringing it to a secure

stop. It is similar in function to the loose gravel on freeway truck escape ramps, but much more costly. The Kanawha Commission President said he expects the cost of repairs to be high. "I can't imagine that it will be less than seven figures, but I don't know that for sure," he said. Officials are hoping to acquire emergency funding from the Federal Aviation Administration to complete the repairs. Afterward, they plan to pursue reimbursement from U.S. Airways or its insurance provider.
Source: http://www.dailymail.com/News/201001200524

22. *January 21, WKYW 1060 Philadelphia* – (Pennsylvania) **Jewish prayer implement leads to emergency landing at PHL.** Officials say a Jewish teenager's tefillin — leather boxes that are strapped to the forearm and forehead during prayers by Orthdox Jews — caused an emergency response Thursday morning when they were spotted by passengers aboard a New York-to-Louisville commuter plane. According to investigators, passengers aboard the flight were alarmed when they saw the devices and notified the plane's crew. The pilot diverted the plane to Philadelphia International Airport, where it was met by emergency security personnel. The young man was removed from the plane for questioning by local and federal law enforcement officials. Police say the 17-year-old Jewish teenager, who was traveling with his 16-year-old sister, never made any threats and was cooperative throughout the incident. At the height of the situation, numerous roads around Philadelphia International Airport were closed as a precaution. No charges were being filed. The US Airways Express commuter plane and its 18 passengers, including the teen and his sister, were eventually allowed to resume their journey.
Source: http://www.kyw1060.com/pages/6170202.php?

23. *January 20, Aviation Week* – (National) **AOPA fears lack of backup for GPS.** The Aircraft Owners and Pilots Association (AOPA) expressed dismay at the decision of the U.S. Coast Guard to terminate the U.S. Loran-C signal beginning February 8, 2010, without a backup plan for the global positioning system. The Coast Guard this month released a special notice of its intent to terminate signals. The fiscal 2010 Department of Homeland Security appropriations bill calls for the elimination of Loran-C funding if the Coast Guard Commandant certifies that the system is not necessary as a backup for other federal navigation uses. AOPA noted that while Loran-C is not now widely used for navigation, an enhanced version, eLoran, has been recommended as a backup system for GPS. "The termination of loran will leave the country without a single national backup system in the event of a GPS outage," AOPA said. "Recent reports have shown that the constellation of satellites is vulnerable to outages and service disruptions," said the AOPA vice president of operations and international affairs. "AOPA has long cautioned against decommissioning loran before a separate navigation system is established as a backup."
Source:
http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=busav&id=news/bav/2010/01/18/09.xml

24. *January 20, Los Angeles Times* – (California) **Two planes bound for Burbank struck by lightning.** Two Southwest Airlines Boeing 737s were struck by lightning during

their flights but landed safely at Bob Hope Airport in Burbank. One flight attendant who complained of pain in her arm was taken to the hospital for examination, authorities said. The airliners, which were flying to Burbank from Sacramento and Oakland, landed at 9:38 a.m. and 9:57 a.m., said a spokeswoman for Southwest Airlines. Both planes were taken out of service to check for possible damage. The spokeswoman said the Sacramento flight carried 69 passengers while the Oakland flight had 81 passengers aboard. She did not know how far the aircraft were from the airport when they were struck by lightning. Federal Aviation Administration regulations require that aircraft components and electrical systems be built to withstand lightning strikes.
Source: http://latimesblogs.latimes.com/lanow/2010/01/two-planes-bound-for-burbank-struck-by-lightning.html

25. *January 20, Associated Press* – (International) **Part of Munich airport closed after security alert.** Part of Munich airport was closed Wednesday as officials searched in vain for a man who left a security checkpoint with a bag containing a laptop after it had triggered an alert for possible explosives. The incident appeared to have been a false alarm triggered by a passenger in a hurry to catch his plane, and who was unaware of what had happened. Part of the airport's Terminal 2 was closed following the incident at 3:30 p.m. local time and hundreds of people were evacuated. The area reopened three hours later. Police had not been able to find or identify the man by mid-evening, but said they were still working on it. An airport security instrument alerted officials to possible explosives as the bag with the man's laptop was being scanned, police said. The man quickly left the scene, carrying the computer into the terminal, they said. Officials had wanted to check the bag again. The impression of officials was that "the passenger likely was in a bit of a hurry, grabbed his luggage and headed off," a federal police spokesman said. Although the security instrument flagged the bag, that "doesn't mean that there are explosives inside," and the alert could have been triggered by something else, the spokesman said. He said the machines are set to be very sensitive. While the man did not necessarily commit any offense, police still want to question him about why he left the security check.
Source: http://www.lcsun-news.com/las_cruces-business/ci_14229813

For more stories, see items **2**, **4**, and **10**

[Return to top]

Postal and Shipping Sector

26. *January 21, Times-Standard* – (California) **Bomb scare leads to evacuation.** Dozens of homes and businesses were evacuated Wednesday afternoon when a suspicious package surfaced at the downtown Arcata FedEx Office store and set authorities on an hours-long, meticulous process of moving the possibly explosive device to a safe location for destruction. The Humboldt County Explosive Ordinance Disposal Team, equipped with a robotic bomb handler, was called to G and 16th streets after the suspicious package was dropped off prepaid with a fake return address. At around 5:30

p.m., the package was put into a huge metal box — meant to withstand explosions — mounted on the back of a trailer, then taken to a safe zone where it could be destroyed. A Humboldt County sheriff's office lieutenant said the package was taken to a piece of private property in the east area of the county. He said the team would use one of several detonation options to "render it safe," then examine the remnants to see if it was an explosive device. That information was not available at deadline.
Source: http://www.contracostatimes.com/california/ci_14236989

[Return to top]

Agriculture and Food Sector

27. *January 20, NBC 4 Columbus* – (National) **Indiana firm recalls frozen chicken pot pie products.** Park 100 Foods, Inc., a Kokomo, Indiana, establishment, is recalling approximately 19,200 pounds of frozen chicken pot pie products that may contain foreign materials, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Wednesday. The product subject to recall includes 2.5-pound cartons of "Market DayÂ®, CHICKEN POT PIE, Made With All White Chicken Meat." Each carton bears a Julian date "28209" which is located on the right side panel, an order number "7138" and the establishment number "P-6882" inside the USDA mark of inspection. The products were produced by Park 100 Foods on October 9, 2009, and were distributed by Market Day through Internet or catalog sales in Delaware, Florida, Illinois, Indiana, Iowa, Kentucky, Maryland, Michigan, Missouri, New Jersey, Ohio, Pennsylvania, Virginia, West Virginia and Wisconsin. The problem was discovered after Market Day received a customer complaint about finding metal straight pins in the product.
Source:
http://www2.nbc4i.com/cmh/news/local/article/indiana_firm_recalls_frozen_chicken_pot_pie_products/30328/

28. *January 20, Hoosier Ag Today* – (National) **Fertilizer industry sees impacts from chemical security bill.** Fertilizer costs and supply could suffer under legislation moving through congress, unless changes are made, according to those inside the fertilizer industry. A Fertilizer Institute spokeswoman says her industry does not oppose continued requirements to do plant terrorism security planning. But requirements in a house-passed bill that the senate has yet to consider that would force product substitution is a different story. "It has been our opinion that inherently safer technologies or product substitution, whatever you want to call it, is not a security issue. It is a safety issue," the spokeswoman said. She added that forcing makers of anhydrous ammonia for fertilizer to switch products would drive up costs and hurt quality. "Our ability to produce a very valuable nitrogen fertilizer, in our opinion, would have a very negative impact on farmer's ability to grow crops."
Source:
http://www.hoosieragtoday.com/wire/news/00148_fertilizerlegislation_223537.php

29. *January 20, Pacific Business News* – (Hawaii) **Drought leaves 99% of Hawaii dry.** Hawaii agriculture continues to be damaged by an unrelenting drought that has continued into the state's rainy season. The weekly crop report by the U.S. Department of Agriculture's Hawaii office for the week ending Jan. 17 found that 99 percent of the state is in a drought, with more than a third of the state in a severe drought with average rainfall well below typical levels. Less than an inch of rain has fallen so far this year at 13 of 17 monitoring stations across the Islands. In an average year, cumulative rainfall amounts between 5 and 14 inches is expected by mid-January. Maui and the Big Island have been especially hard hit by the drought, requiring heavy irrigation to keep crops viable. Some parts of Hawaii are entering their third year of drought, leading to lower yields for thirsty crops like sugar and forcing water restrictions on Maui and parts of the Big Island.
Source: http://pacific.bizjournals.com/pacific/stories/2010/01/18/daily20.html

30. *January 19, U.S. Environmental Protection Agency* – (Washington) **Ocean Protein LLC pays nearly $22,000 for failure to properly report hazardous chemicals.** Ocean Protein, LLC has settled with the Environmental Protection Agency and agreed to pay a $13,166.00 penalty for violating the federal Emergency Planning and Community Right-to-Know Act (EPCRA). The company failed to properly report the storage of Sulfuric Acid at its fish waste processing facility located in Hoquiam, Washington. The company produces fish meal, fish oil, and bone meal from fish wastes using sulfuric acid, among other chemicals. In addition to the penalty, Ocean Protein agreed to provide over $8,800 for training and equipment to the City of Hoquiam Fire Department that will improve the department's capabilities in responding to hazardous materials emergencies in a safe and effective manner.
Source: http://media-newswire.com/release_1110603.html

31. *January 18, Southwest Times Record* – (Arkansas) **Firefighters put out blaze at Tyson plant.** Clarksville firefighters extinguished a blaze in a laundry room at a Tyson plant early Saturday afternoon. Members of the Clarksville Fire Department were called to the factory at 11:58 a.m. after a report that a laundry room at the plant was burning, according to a deputy chief of the fire department. When firefighters arrived, they found smoke and flames, but the fire was limited to the laundry room, which is the only area in the plant without a sprinkler system. Sprinklers in parts of the plant outside of the laundry room prevented the fire from spreading, according to the deputy chief. Firefighters had the blaze under control in 30 to 40 minutes. No one was injured. No one was inside the laundry room, which contains two large gas dryers, when the blaze ignited. How the fire ignited has yet to be determined, he said.
Source: http://www.swtimes.com/articles/2010/01/18/news/news011810_07.txt

[Return to top]

Water Sector

32. *January 20, Oregonian* – (Oregon) **Portland parks group opposes idea to give guns to Water Bureau security.** The Portland Parks Board voted today to oppose the city

commissioner's proposal to give guns and arresting powers to the people who protect Portland's drinking water. The 11-member board, which provides a forum for discussion about park issues, voted unanimously after hearing from the Water Bureau's administrator and the police chief. Currently, 19 security officers and two administrators in the Water Bureau are authorized to patrol the city's open reservoirs and call police for help. The commissioner's proposal would create a law enforcement unit within the bureau whose members would undergo basic training through the Oregon Department of Public Safety Standards and Training. He has argued that police response times vary and his people need backup to protect a valuable public resource. The Water Bureau owns five open reservoirs located in city parks — Mt. Tabor and Washington Park. The Water Bureau's administrator has said the bureau needs a way to handle trespassers, fire-building campers, as well as terrorists capable of harming the city's water supply.
Source:
http://www.oregonlive.com/portland/index.ssf/2010/01/portland_parks_group_opposes_i.html

33. *January 19, Seattle Post Intelligencer* – (Washington) **Seattle's sewers are getting clogged with grease.** It is estimated that 544,000 gallons of grease slip down Seattle's drains each month. Most of it comes from dirty dishes and food waste, and it is a problem. In the last five years, grease-clogged pipes caused about one-third of Seattle's sewer backups, according to Seattle Public Utilities (SPU). From January to October last year, there were 147 such incidents, and that does not count the times when residents called SPU only to discover that the blockage was in the side sewer on their property. "The City of Seattle is really working on getting the word out that it is a problem," said the coordinator of the city's fats, oils and grease program, or what utility workers call "FOG." It's an issue for any city or county with older sewer pipes and residents who consume animal products. Cities have taken various approaches to reducing the amount of grease discharge, either through stepped-up recycling programs or stronger regulations. The City of Seattle prohibits directly dumping grease down the drain and restricts how much grease can be in your wastewater. SPU officials say they're considering stronger regulations on grease-traps and how much FOG can be in wastewater coming from an establishment.
Source: http://www.seattlepi.com/local/414191_grease18.html

34. *January 18, Pryor Daily Times* – (Oklahoma) **Thieves hold up sludge at Salina.** Salina Public Works Authority Board of Trustees voiced their frustrations and concerns regarding the recent theft of trailer wheels and tires from the sewer plant. This is the second time they have been stolen in just over two months. The first theft occurred on Halloween night, according to the town clerk. As a result, the trailer of sludge could not be hauled off as planned. Trustees voted to approve the expenditure of roughly $3,000 to replace the wheels and tires in their December meeting. The wheels and tires were replaced. The wheels were even chained to the trailer to prevent tampering. In the early hours of January 9, with the temperature hovering around four degrees, thieves struck again. The chains were cut, the tires and wheels stolen. The area where the sewer plant is located is very dark at night. PSO has a work order to install

light poles at the facility, but work has not begun. For now, the PWA is facing the expense of replacing the stolen goods, again. “I think we’re going to have to keep them locked up and just put them on the trailer when we need to use it,” the mayor commented.
Source: http://www.pryordailytimes.com/local/local_story_018150423.html

[Return to top]

Public Health and Healthcare Sector

35. *January 21, Bloomberg* – (International) **WHO to clarify H1N1 data after false pandemic claim.** The World Health Organization will clarify data on swine flu after media reports of a false pandemic hindered public health measures, India’s Health Secretary said. Governments from the U.S. to Germany are curbing purchases of vaccine to fight the new H1N1 virus after cases declined and the first flu pandemic in 41 years appeared milder than initially feared. The Parliamentary Assembly of the Council of Europe plans to debate the theme “Faked pandemics: a threat to health” at a plenary session in Strasbourg, France, next week. At the United Nations agency’s executive board meeting in Geneva this week, India’s Health Secretary asked the WHO to explain media reports about a false pandemic, she said yesterday in a statement to India’s Press Information Bureau. The Indian Health Secretary also called for greater transparency about terms and conditions on which international vaccine manufacturers were supplying the shots to countries, according to the statement.
Source: http://www.bloomberg.com/apps/news?pid=20601091&sid=ahj0H_RH8U68

36. *January 20, BBC* – (International) **Drug firm boost to malaria fight.** Pharmaceutical company GlaxoSmithKline is to reveal previously confidential data on thousands of potential anti-malaria compounds. In addition to this, the company is to pump millions into an ‘Open Lab’ for independent research teams. The company has 13,500 molecules which have been tested against the parasite which causes malaria. One expert said more sharing of data could trigger advances like those that came from the human genome project. The way in which pharmaceutical firms guard the secrets of their drugs and research has long been cited as an obstacle to disease research.
Source: http://news.bbc.co.uk/2/hi/health/8470087.stm

[Return to top]

Government Facilities Sector

37. *January 21, Wassau Daily Herald* – (Wisconsin) **Student makes bomb threat.** A Horace Mann Middle School student is accused of writing a bomb threat on a bathroom wall Wednesday, but school officials say the student had no intention of acting on the threat. The Horace Mann principal said students alerted staff members Wednesday morning that a bomb threat was written on an eighth-grade boys’ bathroom wall. The writing made reference to a bomb and an incident that would take place at the school Wednesday, he said. The student who made the threat was identified based on

information provided by students and video from security cameras, the principal said. No evacuations took place and students and staff members never were in danger, he said. The principal credited students for quickly alerting staff members of the threat. A letter was sent home with Horace Mann students to inform parents about the incident. The Wausau police chief said the student was released to the student's father and was referred to juvenile services on a charge of making a bomb threat.
Source:
http://www.wausaudailyherald.com/article/20100121/WDH0101/1210657/1581&located=rss

38. *January 21, Tallahassee Democrat* – (Florida) **TPD probes bomb threat at Raa, Springwood schools.** No arrest has been made and Tallahassee police are continuing to investigate a bomb threat that occurred Wednesday morning at two Leon County schools. Principals at Raa Middle and Springwood Elementary schools were forced to evacuate staff and students between 8:45 a.m. and 9 a.m. Wednesday when they were informed by district administrators of a bomb threat. The threat came in the form of a 911 call to TPD dispatchers. Police were able to trace the call to the Express Lane convenience store at 2784 West Tharpe St., which is at the intersection of Mission Road. Crime scene investigators pulled finger prints from the phone, and investigators ruled out one person who had used the phone prior to the call, a TPD police spokesman. The spokesman said investigators reviewed store surveillance videotape but were unable to find anything. Located just a block from North Monroe Street at Tharpe Street and North Martin Luther King Jr. Boulevard, Raa Middle School had not yet begun its day when the principal was notified at about 8:45 a.m. Because the 880 enrolled students were not yet in the building, the principal had to evacuate a staff of about 70. Students who were being dropped off by parents and school buses were directed to the bus drop-off while the sweep was being conducted.
Source: http://www.tallahassee.com/article/20100121/NEWS0102/1210321/1001/RSS

39. *January 20, Minnesota Daily* – (Minnesota) **Chemical spill causes Shepherd laboratories evacuation.** An acid spill in the University of Minnesota Shepherd laboratories on Union Street SE caused emergency responders to close a floor of the building last night. Approximately two liters of hydrochloric acid were spilled in the hallway near one of the labs on the fourth floor of the building, said a University Environmental Health and Safety public health specialist. Four people involved in the spill, including two who were in the lab, were brought by an ambulance to a University hospital as a precaution, according to a spokesman for the Minneapolis fire department. However, they did not appear to be injured. "This is kind of a medium to small event on the scale of spills around the University," the public health specialist said. "I mean, its research. Stuff happens." A 911 call reporting a smell alerted emergency responders to the situation. About a dozen fire, police and emergency vehicles responded and lined Union Street. The acid was of unknown strength. Firefighters deposited soda ash on the chemical to neutralize it, and closed the floor.
Source: http://www.mndaily.com/2010/01/20/chemical-spill-causes-shepherd-laboratories-evacuation

40. *January 20, First Coast News* – (Florida) **Jacksonville City Hall evacuated due to bomb scare.** Jacksonville Police closed streets downtown after a bomb scare. Hours later, they were at the scene of a second suspicious object nearby. Jacksonville Sheriff's Officers said a black suitcase was found lying on the sidewalk near Church and Laura Streets just before 5 p.m. Police cleared the area. At one point, the sheriff's office was so concerned they pushed the media about a block away from Hemming Plaza, which is in front of City Hall. Officers said the plaza was considered a "blast area," in case the suspicious object detonated. As darkness set in and the investigation continued, several downtown employees told First Coast News they were stranded. The bomb squad had restricted access to area parking garages.
Source: http://www.firstcoastnews.com/news/local/news-article.aspx?storyid=151012&provider=rss

41. *January 20, Minnesota Daily* – (Minnesota) **Chemical spill causes Shepherd laboratories evacuation.** An acid spill in the University of Minnesota Shepherd laboratories on Union Street SE caused emergency responders to close a floor of the building the evening of January 19. Approximately two liters of hydrochloric acid were spilled in the hallway near one of the labs on the fourth floor of the building, said a University Environmental Health and Safety public health specialist. Four people involved in the spill, including two who were in the lab, were brought by an ambulance to a University hospital as a precaution, according to a spokesman for the Minneapolis fire department. However, they did not appear to be injured. A 911 call reporting a smell alerted emergency responders to the situation. About a dozen fire, police and emergency vehicles responded and lined Union Street. The acid was of unknown strength. Firefighters deposited soda ash on the chemical to neutralize it, and closed the floor."It's a little more serious because it was out in the hallway and then we have less control of where the chemical vapors go," the specialist said, "but it's confined to the floor, it's something you can neutralize, and the firefighters have neutralized it."
Source: http://www.mndaily.com/2010/01/20/chemical-spill-causes-shepherd-laboratories-evacuation

[Return to top]

Emergency Services Sector

42. *January 21, Associated Press* – (Vermont) **Vt. depts. get recruiting funding.** Volunteer first responders across Vermont will be getting some help finding new members and training those who are already serving, a U.S. Senator from Vermont said Monday. The Senator announced a $100,000 grant that will encourage service on volunteer fire departments and other first response organizations through improved outreach to high school students, a continuation of a successful summer program for young people and other efforts. "Vermont is deeply indebted to our volunteer first-responder community, and we've got to do everything we can to maintain their ranks," said the Senator during a news conference at his Burlington office where he announced the grant. The Senator was joined by firefighters from across Vermont and the president of the American Ambulance Association. The Senator cited a report by the

U.S. Fire Administration that says volunteer emergency services are a "tradition in danger of weakening and possibly even dying out." Since 1984 the number of volunteers across the country has dropped by more than 97,000 people. A separate survey by he National Fire Protection Association showed that at least two-thirds of the nation's fire departments are understaffed. And the situation is worse in rural communities.
Source: http://www.firehouse.com/topic/training/vt-depts-get-recruiting-training-funding

43. *January 20, Fort Wayne Journal Gazette* – (Ohio) **Ambulance fire clears Defiance offices.** Municipal offices in Defiance, Ohio, were briefly evacuated Tuesday after firefighters noticed an ambulance was on fire at a fire station. The fire was reported about 2:30 p.m. in the fire station, 702 W. Third Street. Firefighters were alerted to a loud pop and hiss in the fire department's apparatus bay. An ambulance that was plugged into a battery to charge the truck, officials said, and its equipment caught fire. Firefighters were able to contain and extinguish the blaze. Municipal offices attached to the fire department were evacuated for about 45 minutes, officials said. The cause of the blaze is under investigation by the Ohio State Fire Marshal's office.
Source: http://www.journalgazette.net/article/20100120/LOCAL07/301209937/1002/LOCAL

44. *January 19, U.S. Government Accountability Office* – (National) **GAO-10-41, Information Sharing: Federal agencies are sharing border and terrorism information with local and tribal law enforcement agencies, but additional efforts are needed.** GAO has recommended that DHS and the FBI more fully identify the information needs of and establish partnerships with local and tribal officials along the borders; identify promising practices in developing border intelligence products within fusion centers and obtain feedback on the products; and define the suspicious activities that local and tribal officials in border communities are to report and how to report them. DHS agreed and the FBI did not comment.
Source: http://www.gao.gov/htext/d1041.html

[Return to top]

Information Technology Sector

45. *January 21, Computerworld* – (International) **Microsoft confirms 17-year-old Windows bug.** Microsoft late on January 17 issued its second advisory of the last week, warning users that a 17-year-old bug in the kernel of all 32-bit versions of Windows could be used by hackers to hijack PCs. The vulnerability in the Windows Virtual DOS Machine (VDM) subsystem was disclosed on January 19 by a Google engineer on the Full Disclosure security mailing list. Coincidentally, the engineer received credit for reporting the single vulnerability that Microsoft fixed last week on its regular Patch Tuesday. The VDM subsystem was added to Windows with the July 1993 release of Windows NT, Microsoft's first fully 32-bit operating system. VDM allows Windows NT and later to run DOS and 16-bit Windows software. The January

20 advisory spelled out the affected software — all 32-bit editions of Windows, including Windows 7 — and told users how to disable VDM as a workaround. Windows' 64-bit versions are not vulnerable to attack.
Source:
http://www.computerworld.com/s/article/9146820/Microsoft_confirms_17_year_old_Windows_bug

46. *January 20, The Register* – (International) **Adobe fixes critical Shockwave bugs with neanderthal patch.** The critical patches for Adobe Systems software keep coming. This time, they fix serious security bugs in the company's Shockwave Player. Adobe on on January 20 pushed out updates for Shockwave 11.5.2.602 and earlier on Windows and Mac operating systems. The patches fix multiple integer overflow and buffer overflow flaws that can be exploited to execute malicious code on computers that use the software. Adobe is strongly urging users to upgrade. Unlike the vast majority of today's patches, the Shockwave fix requires users manually uninstall the out-of-date version, reboot their systems, and then install the latest version. More importantly, making it inconvenient for users to upgrade is a guarantee that a sizable portion of them will remain vulnerable. Adobe has recently unveiled an automatic updater for its Reader application.
Source: http://www.theregister.co.uk/2010/01/20/critical_adobe_shockwave_bugs/

47. *January 20, DarkReading* – (International) **Researcher: Flaws in Facebook app authorization could lead to clickjacking.** Vulnerabilities in the way members authorize the use of third-party applications in Facebook could potentially lead to loss of personal information or even targeted attacks on specific individuals, a security researcher said on January 20. A well-known security researcher and author of Hacking: The Next Generation, says he has discovered design flaws in Facebook that could allow attackers to collect the personal information of users on the social networking site, and even build profiles of "friends" that might facilitate direct attacks on specific individuals within a company. The flaws were presented to Facebook in November; the researcher has agreed not to release specific code or other details for two weeks while technical staffers at the social networking site continue their efforts to patch the vulnerabilities. The researcher says he has begun to speak generally about the problem, with Facebook's permission. The vulnerabilities center around the way Facebook enables users to place third-party applications on their social networking pages, the researcher says.
Source:
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=222301736

48. *January 20, IDG News Service* – (International) **'Sudden failure' Wednesday morning brings Twitter down.** On the morning of January 19, Twitter suffered a "sudden failure" and then encountered problems switching to a backup system, which left the site "largely inaccessible" for about 90 minutes, the company said. Once notorious for regular and prolonged outages, Twitter has improved in this respect in the past year, but remains inconsistent. In August of last year, Twitter logged more than 6

hours of downtime, following a total of only 17 minutes in July, according to monitoring company Pingdom. In October, it had more than 5 hours of downtime, sandwiched between only 33 minutes in September and 22 minutes in November.
Source: http://www.computerworld.com/s/article/9146680/_Sudden_failure_Wednesday_morning_brings_Twitter_down

49. *January 20, The Register* – (International) **BOFH-making bug plugged in D-link update.** D-Link has plugged a security vulnerability involving protocol handling by some of its wireless routers that creates a potential means for normal users to grab super-user privileges. The network manufacturer issued a firmware update that addresses a recently discovered bug in how its networking devices handle the Home Network Administration Protocol (HNAP). The flaw meant that the devices offered a shadow connection outside of the regular administrative access channel. This permanent unauthorised connection might be exploited by miscreants to assume admin privileges and change router settings, and might also be used to bypass CAPTCHA login features introduced by D-Link in recent firmware upgrades. Successful exploitation requires valid login credentials, so the flaw is a privilege elevation risk rather than something more serious. The security shortcoming was found by SourceSec and covered by D-Link with an advisory on January 18. Only some of D-Link's routers are vulnerable. The networking manufacturer issued updates for its DIR-635, DIR-655 and DIR-855 routers. Discontinued DIR-615, DI-634M and DIR-635 models are also at risk. An update for the DIR-615 is already available, with updates for the DI-653-M and DIR-635 promised for upcoming weeks.
Source: http://www.theregister.co.uk/2010/01/20/d_link_security_update/

50. *January 19, Computerworld* – (International) **Researchers up ante, create exploits for IE7, IE8.** Researchers have created attack code that exploits a zero-day vulnerability in Internet Explorer 7 (IE7) as well as in the newest IE8 — even when Microsoft's recommended defensive measure is turned on. Microsoft, however, continues to urge users to upgrade from the eight-year-old IE6 — the only version yet successfully attacked in the wild — to the newer IE7 or IE8. On January 17 a security vulnerability researcher and co-author of The Mac Hacker's Handbook, crafted attack code that exploits the unpatched vulnerability in IE7 when it's running on either Windows XP or Windows Vista. "And now my Aurora exploit works on IE7 on Vista as well as IE6, IE7 on XP. Remember kids, DEP is useless if the app doesn't opt in," said the researcher on Twitter. "My version [of the exploit] implements a different heap manipulation algorithm," said the researcher in a telephone interview on January 19. "It works on IE7 on XP and Vista because the browser doesn't opt in on DEP [data execution prevention]." In fact, said the researcher, even the newest IE8 is not safe from attack if it's running on Windows XP Service Pack 2 (SP2) or earlier, or on Windows Vista RTM (release to manufacturing), the version Microsoft shipped in January 2007.
Source: http://www.computerworld.com/s/article/9145958/Researchers_up_ante_create_exploits_for_IE7_IE8

51. *January 19, SC Magazine* – (International) **iDefense retracts claims made on Adobe's involvement in cyber attacks.** Security firm iDefense has withdrawn a comment made earlier about the Google attack. As published on the SC Magazine website on the 13th January, the iDefense head of international cyber intelligence claimed that 'attackers delivered malicious code used against Google and others using PDFs as email attachments', similar to an attack in July 2009 which employed a PDF file that exploited a zero-day vulnerability in Adobe Reader. However in a blog update on the Adobe website, iDefense has issued a statement retracting the comment. It said: "In iDefense's press announcement regarding the recently discovered Silicon Valley compromises, we stated that the attack vector was likely 'malicious PDF file attachments delivered via email' and suggested that a vulnerability in Adobe Reader appeared to have been exploited in these attacks. "Upon further review, we are retracting our initial assessment regarding the likely use of Adobe vulnerabilities. There are currently no confirmed instances of a vulnerability in Adobe technologies being used in these attacks. We continue to investigate this issue."
Source: http://www.scmagazineuk.com/idefense-retracts-claims-made-on-adobes-involvement-in-cyber-attacks/article/161661/

52. *January 19, New York Times* – (International) **Fearing hackers who leave no trace.** The crown jewels of Google, Cisco Systems or any other technology company are the millions of lines of programming instructions, known as source code, that make its products run. If hackers could steal those key instructions and copy them, they could easily dull the company's competitive edge in the marketplace. More insidiously, if attackers were able to make subtle, undetected changes to that code, they could essentially give themselves secret access to everything the company and its customers did with the software. The fear of someone building such a back door, known as a Trojan horse, and using it to conduct continual spying is why companies and security experts were so alarmed by Google's disclosure recently that hackers based in China had stolen some of its intellectual property and had conducted similar assaults on more than two dozen other companies. "Originally we were saying, 'Well, whoever got it has the secret sauce to Google and some 30 other California companies, and they can replicate it,' " said a director of security intelligence at VeriSign iDefense, which helped Google investigate the Chinese attacks. "But some of the more devious folks in our outfit were saying, 'Well, they could also insert their own code — and they probably have.' "
Source: http://www.nytimes.com/2010/01/20/technology/20code.html

53. *January 19, IDG News Service* – (International) **Study: Click fraud rate relatively low in 2009's Q4.** Click fraud, a practice that dilutes the efficacy of pay-per-click (PPC) advertising campaigns run in search engines like Google, stayed relatively low in the fourth quarter, according to a study. Click Forensics, a provider of click-fraud detection services and products, said on January 19 that the industry's average click-fraud rate for the quarter ending December 31 was 15.3 percent. Although that is up from the 14.1 percent rate in the third quarter, it also represents a significant drop from 2008's fourth quarter, when the click-fraud rate hit an all-time high of 17.1 percent. Click Forensics credited search engines, Web publishers and ad networks with doing a

better job of detecting click fraud in the commerce-heavy holiday season.
Source:
http://www.computerworld.com/s/article/9145998/Study_Click_fraud_rate_relatively_low_in_2009_s_Q4

For another story, see item **18**

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

54. *January 21, Denver Post* – (National) **FCC plans to expand limits on "robocalls".** A federal agency wants to make it easier for consumers to avoid getting automated telephone solicitations unless they want them. The proposed rules announced on January 20 by the Federal Communications Commission (FCC) shore up regulations on businesses that rely on prerecorded telemarketing calls — referred to as "robocalls" — and makes it harder for them to pester consumers. "It's certainly a step in the right direction as the vast majority of the public would love to get rid of all robocalls," the Colorado attorney general said. The FCC rules apply to industries not covered by similarly restrictive rules issued last year by the Federal Trade Commission (FTC) — telephone companies, airlines, banks, and insurance companies. Companies would have to obtain a consumer's written approval for the telephone pitches. Most businesses that use prerecorded sales calls — such as the automobile-warranty companies that peppered the state with calls last year — are subject to the FTC rules. The FCC rules bring in those industries not covered by the FTC. The FCC must take public comment before making the rules permanent.
Source: http://www.denverpost.com/business/ci_14234066

55. *January 20, KITV 4 Honolulu* – (Hawaii) **22,000 Kauai Hawaiian Telcom customers lose service.** A contractor working on Kauai on January 20 cut fiber optic lines that cut phone and data service to about 22,000 customers, Hawaiian Telcom said. The outage began at about noon when the contractor working on Wailua Bridget cut the lines, a Hawaiian Telcom spokeswoman said. The outage affected 17,000 voice customers and 5,000 data customers from Princeville to Kappa, she said. Customers also reported problems in the Kalaheo area, the spokeswoman said. The county urged people needing to call 911 to use their cellular phones, but Hawaiian Telcom said that some carriers have also been impacted. Hawaiian Telcom said that crews would gradually restore service at about 5 p.m.
Source: http://www.kitv.com/money/22297915/detail.html

56. *January 20, Torrance Daily Breeze* – (California) **Cable damage knocks out Verizon service in Rolling Hills.** Dozens of Verizon customers in Rolling Hills are without phone service on January 20 after an underground cable line was damaged, possibly due to a storm-related power outage on January 19. The company has so far had 57 reports of trouble, but many more are likely affected. The outage is in the Amaga Springs Road and High Ridge Road areas. Crews are working to excavate the cable, but rainy weather is making repair efforts difficult, said a spokesman with the phone company. "We will be working around the clock until service is restored," he said. Source: http://www.dailybreeze.com/news/ci_14230112

57. *January 20, Press-Enterprise* – (California) **Murrieta puts hold on cell towers.** Murrieta is putting the brakes on requests to build new cell phone towers in the city. The City Council recently agreed to stop accepting new requests to build the towers so officials can study the need for new regulations. Demand for cell towers is expected to increase in the coming years with demand exploding for mobile Internet service used by laptops and smartphones like Apple's iPhone. The city's public works director told the council that Murrieta has several active requests from companies seeking to build new wireless towers. Many more are expected in the near future, he said. He did not say where companies were proposing to build the new towers. New cell phone towers are commonly built to blend in with their surroundings, in such guises as trees and flagpoles. In many cases they are approved with little problem. But towers put in residential areas can be a different story. Murrieta's regulations need to be revamped because they were written in 1997, before many advancements in wireless technology, the director said. They also apply only to towers built on private property. Source: http://www.pe.com/localnews/inland/stories/PE_News_Local_W_scell21.4673c1d.html

[Return to top]

Commercial Facilities Sector

58. *January 20, Associated Press* – (Texas) **Feds probing rash of church fires in East Texas.** Federal authorities are investigating a rash of church fires in East Texas, where seven such blazes have been reported since January 1. Police said the latest Tyler-area fire at Bethesda House of Prayer in Lindale was quickly contained Wednesday morning. No injuries or deaths have been reported. The Lindale fire came after two weekend church fires in Tyler, about 100 miles east of Dallas. Authorities have not said the fires are linked, or whether arson was the cause. Agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives moved in last week after three church fires were reported over 12 days in nearby Athens. The Athens blazes caused officials to re-examine a church fire in Canton, 40 miles west of Tyler.
Source: http://www.dallasnews.com/sharedcontent/APStories/stories/D9DBJ2PO0.html

59. *January 20, KJCT 8 Grand Junction* – (Colorado) **Choice Hotels receives bomb threat.** In the wake of a long string of office violence — Grand Junction, Colorado,

police say they responded to a bomb threat at Choice Hotels call center. Early this afternoon the center received an anonymous bomb threat. Police arrived on scene and spoke with management. Police say the Choice Hotels manager wasn't concerned the threat was for real. After a search — police found no traces of a bomb and were unable to trace the call. They have no suspects at this time and are not opening an investigation.
Source: http://www.kjct8.com/Global/story.asp?S=11846798

60. *January 20, Eureka Times-Standard* – (California) **Bomb scare: Portions of Arcata's North Town evacuated.** A suspicious package — just a little bigger than a shoebox — that was dropped off at Kinko's this afternoon and led to evacuations throughout North Town is now in the hands of the Humboldt County, California, bomb squad, which will take the package to a disposal site to determine if it is an explosive device. The one-square-block portion of downtown Arcata has been reopened so that residents and business owners and employees can return to their properties. Authorities have X-rayed the parcel, and still believe it to be suspicious, according to officials on scene at about 4:30 p.m. The bomb squad was deployed there late this afternoon. After examining the package, they too determined it suspicious and widened the safety perimeter, officials with the Arcata Fire Protection District (AFPD) said. Impacted businesses included Hey Juan Burritos, Hutchins Grocery, and Wildflower CafÃ©, among others. The first call came in to the AFPD at around 1:17 p.m. The package is marked with a fictitious return address and was apparently destined for the Berkeley area. Officials say they have surveillance footage of the person who dropped the package off.
Source: http://www.times-standard.com/ci_14232964?source=most_viewed

[Return to top]

National Monuments and Icons Sector

61. *January 20, Christian Science Monitor* – (Washington) **Mt. Rainier's retreating glaciers are making a mess.** The fallout from Mt. Rainier's shrinking glaciers is beginning to roll downhill, and nowhere is the impact more striking than on the volcano's west side. As receding glaciers expose crumbly slopes, vast amounts of gravel and sediment are being sluiced into the rivers that flow from the Northwest's tallest peak. Much of the material sweeps down in rain-driven slurries called debris flows, like those that repeatedly have slammed Mt. Rainier National Park's Westside Road. "The rivers are filling up with stuff," a park service geologist says. Inside park boundaries, rivers choked with gravel are threatening to spill across roads, bump up against the bottom of bridges and flood the historic complex at Longmire.
Source: http://www.csmonitor.com/Environment/2010/0120/Mt.-Rainier-s-retreating-glaciers-are-making-a-mess

[Return to top]

Dams Sector

62. *January 20, Victorville Daily Press* – (California) **Dam breaks at Mojave Narrows Regional Park.** The dam that holds Horseshoe Lake at Mojave Narrows Regional Park has been breached, draining the lake by about seven feet, officials said on January 20. "We're evaluating the damage," said the chief of staff for 1st District Supervisor. "The water's still flowing through there." The water from Horseshoe Lake is draining into the Mojave River, he said, but no people or properties seem to be in danger. The county had closed Mojave Narrows Regional Park in Victorville on Tuesday due to heavy rain.
Source: http://www.vvdailypress.com/articles/regional-16844-breaks-victorville.html

63. *January 20, Orange County Register* – (California) **U.S. Army Corps releases local dam water.** Flood-control workers at Brea, Fullerton, and Prado dams released water from them this morning to prevent any danger of overflowing as more rains move into the region, the U.S. Army Corps of Engineers said. "Usually, the basins behind the dams are empty, and if water gets to a certain height, it is sent over the spillway," said a spokesman. "There is no danger to residents unless there is an exceptional deluge and the water couldn't be released fast enough." At Fullerton Dam, 18 cubic feet per second was released; at Brea Dam, 46 cubic feet per second; and at Prado Dam, 2,390 cubic feet per second. He said each dam's water capacity is measured in acre feet, which amounts to one acre of land under one foot of water. Fullerton Dam can hold 764 acre feet; Brea, 3,880; and Prado, 174,000.
Source: http://www.ocregister.com/news/dam-230023-water-feet.html

64. *January 20, New Orleans Times-Picayune* – (Louisiana) **Levee leak probed on Mississippi River at Elmwood.** Officials are investigating a levee seepage site along the Mississippi River in Elmwood to figure out why water is leaking onto River Road. An Army Corps of Engineers supervisor said the agency does not think the water is coming from the river itself but instead originates from a stagnant pond in a low section of batture near Powerline Drive, just downriver from the Harahan city limits. Representatives of the corps, East Jefferson Levee District and the property owner met at the site Wednesday to determine how to best drain the batture area into the river. Levee officials had hoped that drainage work would start immediately, but a corps representative said regulatory procedures must be followed to ensure that the process does not compromise levee integrity. Levee District representatives said the property owner will continue to pump some of the standing water into the river until a permanent plan is devised. In the meantime, it continues to leak through the levee and wet an estimated 1,000-foot stretch of River Road.
Source:
http://www.nola.com/politics/index.ssf/2010/01/levee_leak_probed_on_mississip.html

65. *January 20, Indian Valley News* – (California) **Roadbed on Round Valley Dam cracks.** California State officials asked Indian Valley Community Services District personnel to monitor cracks in the roadbed on the Round Valley Reservoir Dam after a recent inspection. The cracks show some movement there, reported the Water operations manager, though he did not seem unduly concerned. His main concern was the possibility of not being able to place the boards across the dam when it comes time to raise the reservoir level in the spring and summer months. He reported these

concerns to directors during their regular meeting Wednesday, January 13. He was asked to monitor the cracks for several weeks, to see exactly how much movement there is over a period of time, and then he will talk with the inspector again. One way to determine if there is movement is to paint marks on existing cracks in the road, he said. “Any additional cracks in the road could indicate that the top of the dam is moving,” he continued. Monitoring points have been installed along the crest of the dam, which will be surveyed at regular intervals. Surveys will be more frequent until there is enough accurate information to determine if any action is needed. The reservoir level has remained high this year, 20 percent higher than in previous years. Losses due to leaks and old meters were 14 million gallons less than last year, and sales increased by about 6 million gallons. This is the first year more water has been sold than lost.
Source: http://www.plumasnews.com/index.php/home/6552-roadbed-on-round-valley-dam-cracks

[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