Homeland Security

Daily Open Source Infrastructure Report for 25 November 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to the San Francisco Examiner, water officials are rushing to repair a massive pipe, one of the two pipes that carry drinking water into an out-of-service reservoir, to ensure the eastern half of San Francisco continues to have clean water. (See item **18**)
- The Register reported that a bug in Microsoft's Internet Explorer browser is causing more than 50 million files stored online to leak potentially sensitive information that could compromise user privacy, a security researcher said. (See item **28**)

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. *November 23, Associated Press* – (Ohio) **Oil mist released from Ohio refinery.** An Ohio refinery is recommending that nearby residents toss out food, including pet food, that may have come in contact with oil mist accidentally discharged over the weekend. Husky Energy Inc. also is offering car washes to people in northwest Ohio whose vehicles were coated by the mist, released at 9:45 a.m. on November 22 from a storage tank at the company's facility in Lima. Husky said in a statement that it does not

believe the mist is harmful to people or animals and that any residue can be removed with soap and water. A spokesman for the Calgary, Canada-based company, says a safety valve released excess pressure, as it was designed to do. But he says Husky is investigating why some things did not happen before that point.
Source: http://www.rdmag.com/News/FeedsAP/2009/11/energy-oil-mist-released-from-ohio-refinery/

For another story, see item **17**

[Return to top]

Chemical Industry Sector

2. *November 23, Reuters* – (Texas) **Train with petcoke, chemicals derails in Houston.** A Union Pacific (UP) Corp train derailed Monday, sending 16 carloads of petroleum coke off the tracks and spilling much of the cargo, a UP spokeswoman said. No one was hurt in the derailment late Monday morning on the south side of Houston, the UP spokeswoman said. The train, which also carried polyethylene, ammonium nitrate and railroad wheels, was headed from Houston to San Antonio.
Source: http://www.reuters.com/article/domesticNews/idUSTRE5AM3PF20091123

3. *November 23, Mooresville Tribune* – (North Carolina) **Mooresville waste station reopens after chemical incident injures 2.** The Mooresville Waste Transfer Station reopened Monday afternoon following a morning chemical-disposal incident that injured two sanitation workers and shut down the facility. About 10:30 a.m., two Town of Mooresville employees received minor burns when acid-based materials in a residential trash can on Boger Street created a small explosion as they were collected and compressed in a garbage truck. A Mooresville Fire Battalion Chief said town firefighters and the Mooresville Hazardous Materials squad were called to the scene. Additional contamination occurred at the transfer station on N.C. 150 when the town garbage truck was unloaded. To neutralize the chemical waste there and in the truck, a special cleanup company was brought in. The transfer station reopened to the public by 4:30 p.m. Monday. In a news release, the chief said the two injured workers were treated for minor burns and released. The director of solid waste for Iredell County said that “whoever disposed this material made a mistake.”
Source: http://www2.mooresvilletribune.com/content/2009/nov/23/mooresville-waste-station-reopens-after-chemical-i/

[Return to top]

Nuclear Reactors, Materials and Waste Sector

4. *November 24, Reuters* – (Pennsylvania) **FirstEnergy Pa. Beaver Vly 2 reactor in hot shutdown.** FirstEnergy Corp.’s 846-megawatt Unit 2 at the Beaver Valley nuclear power station in Pennsylvania was in hot shutdown on November 24, the company told the U.S. Nuclear Regulatory Commission (NRC) in a report. The unit shut for refueling

and maintenance by October 12. The company made the report due to an unidentified leakage greater than 25 gallons per minute in the reactor coolant system. The company declared an unusual event, the lowest of the NRC's four emergency classifications, due to the leak. Electricity traders guessed the unit had been close to exiting the refueling outage at the time of the leak. The traders also noted the NRC would likely take this event seriously because the residual heat removal system was one of the last lines of defense to keep the core cool. The leak was into the pressurizer relief tank during the shutdown of one of the trains in the residual heat removal system. The company stopped the leak by isolating the train. The company said in the report the containment was closed and the leak did not cause any radiation to be released.
Source: http://www.reuters.com/article/companyNews/idUSN2429341120091124

5. *November 24, Nuclear Power Industry News* – (National) **Audit Of NRC's physical security inspection program for category I fuel cycle facilities.** The Office of the Inspector General's (OIG) audit report titled, "Audit of NRC's Physical Security Inspection Program for Category I Fuel Cycle Facilities (OIG-10-A-01)," was released on November 23. The report presents the results of the audit of security at Category I facilities; which identifies them as high importance facilities. The main objective of NRC's oversight program for Category I fuel cycle facilities is to ensure that these facilities operate safely and securely in accordance with NRC requirements. Since the terrorist attacks of September 11, 2001, NRC has issued licensees new requirements and guidance to enhance security at Category I fuel cycle facilities against sabotage and theft of nuclear material. The objective of this audit was to assess the effectiveness of the NRC's physical security inspection program over the protection and control of special nuclear material at Category I fuel cycle facilities. Audit of NRC's Physical Security Inspection Program for Category I Fuel Cycle Facilities ii. The assessment held that the Office of Nuclear Security and Incident Response fulfills its responsibility to conduct physical security inspections at Category I fuel cycle facilities. However, the inspection program faces the following two challenges: The need to provide physical security training for supervisors without previous security experience to enhance management oversight of inspections; and the need for Inspection guidance to undergo periodic review to ensure that it aligns with current NRC security guidance and requirements. This report makes two recommendations to improve the agency's physical security inspection program at Category I fuel cycle facilities.
Source: http://nuclearstreet.com/blogs/nuclear_power_news/archive/2009/11/24/audit-of-nrc-s-physical-security-inspection-program-for-category-i-fuel-cycle-facilities-11246.aspx

6. *November 24, Augusta Chronicle* – (Georgia) **Radiation report calls SRS 'exemplary '.** Radiation exposure levels at Savannah River Site increased about 20 percent during 2008, in part because of low flows in the Savannah River, according to the site's annual environmental report. The 310-square-mile site was still characterized as "exemplary" on environmental compliance, with average exposure levels remaining at a small fraction of the allowable standard. The report, using calculations prepared by Savannah River National Laboratory, notes that the largest radiation dose a "maximally exposed individual" could have received from SRS operations in 2008 was estimated to be 0.12

millirem — a 20 percent increase over the 0.1 millirem calculation for 2007. In 2006, the figure was 0.2 millirem, and in 2005 it was 0.13 millrem. A millirem is a standard unit of measure for radiation exposure. The levels recorded in all four years remain less than 1 percent of the Department of Energy's standard of 100 millirem per year, the report said. Levels have generally declined in recent decades as many of the processes that created radiation have ceased or been reduced. "The 2008 all-pathway dose was more than the 2007 dose primarily because of the drought-induced record low Savannah River flow rate in 2008, which resulted in less dilution," the report said. When calculating exposures, scientists use a "maximally exposed individual," a person who spends 24 hours a day wherever the air is worst at the site's boundary, drinks 2 liters of water daily and eats food grown with water from the site.
Source: http://chronicle.augusta.com/stories/2009/11/24/met_556912.shtml

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

7. *November 24, Aerospace Daily and Defense Report* – (Texas) **More JSF test planes, software work needed.** The Pentagon is considering adding more flight test assets and software engineers to the $300 billion F-35 Joint Strike Fighter (JSF) program to avoid major delays to fielding the stealthy, single-engine aircraft. A Joint Estimate Team, consisting of career cost estimators and program evaluators, has found the Lockheed Martin F-35 program is at least $16 billion over its project cost, and achieving the current flight test schedule is unlikely. During a roundtable with reporters on November 23, the Pentagon's acquisition czar said more flight test aircraft would help to conduct the extensive test program in a "compressed period of time." Another possibility is to add more software engineers, perhaps a shift of them, to "block and tackle" issues with the many lines of code needed to operate the aircraft and its mission systems, he says. In past years, the Pentagon has actually removed two aircraft from the flight test program, citing confidence in the ability for Lockheed Martin to use modeling and simulation to validate the design. It is unclear whether this potential plan to add test aircraft signals a risk mitigation strategy or a concern that modeling and simulation will not suffice for some of the workload that it was to address.
Source: http://www.aviationweek.com/aw/generic/story.jsp?id=news/F35112409.xml&headline=More JSF Test Planes, Software Work Needed&channel=defense

8. *November 23, Defense News* – (National) **Presidential helo restart possible next spring.** U.S. Defense Department officials hope to relaunch by next spring a multibillion-dollar effort to design and build a new fleet of helicopters devoted to

ferrying U.S. presidents, the Pentagon's top weapons buyer, said November 23. The Defense Secretary in April terminated the years-long, multibillion-dollar VH-71 effort, citing requirements creep, which refers to the costly and time-consuming practice of adding more and more requirements to new weapon plans. Since then, numerous Defense Department and federal agencies have been working toward a fresh slate of requirements that are more technically feasible than the now-canceled VH-71 program. Pentagon officials have "been working intensively with the White House through the requirements" for a new fleet of presidential transporters, the Pentagon weapons buyer told reporters during a Pentagon roundtable. He said officials are adamant about avoiding the "piling on" of more and more requirements to the package of specs for the new choppers, which many officials and analysts say made the VH-71 program too costly for the Defense Secretary's liking.
Source: http://www.defensenews.com/story.php?i=4389511&c=AME&s=AIR

[Return to top]

Banking and Finance Sector

9. *November 24, CNN* – (National) **Bank 'problem' list climbs to 552.** Despite the frenetic pace of bank failures this year, 552 banks are still at risk of going under, according to a government report published Tuesday. The Federal Deposit Insurance Corp. (FDIC) said that the number of lenders on its so-called problem list climbed to its highest level since the end of 1993. At that time, the agency red-flagged 575 banks. Mounting bank failures have proven costly for the FDIC, an agency created to cover the deposits of consumers and businesses in the event that a bank is shut down. On Tuesday, the agency revealed its deposit insurance fund slipped into the red for the first time since 1991. At the end of the quarter on September 30, the value of the fund was $8.2 billion in the hole. But that number accounts for $21.7 billion the agency has set aside in anticipation of future bank failures. The ongoing recession has already claimed 124 banks this year. But fears persist that the number will multiply in coming years because banks are still taking losses on mortgage-related loans and face growing problems with commercial real estate. The banks that end up on the problem list are considered the most likely to fail because of difficulties with their finances, operations or management. Still, history has shown just 13% of banks on the list have failed on average.
Source: http://money.cnn.com/2009/11/24/news/companies/fdic_list/index.htm

10. *November 23, WFAA 8 Dallas-Fort Worth* – (National) **Electronic pickpocketing threatens credit cards, passports.** Thousands of travelers and consumers can fall victim to electronic pickpocketing and never even know it because they carry new credit cards and U.S. passports. Credit card issuers, along with the U.S. State Department, have begun installing radio frequency identification (RFID) chips in credit cards and passports because the technology holds more data than magnetic stripes and can be read quicker. But, that convenience, experts warn, can also put people at risk of having their information taken. RFID chips are commonly found in cards used to raise gates in parking garages and unlock doors at businesses. All one has to do is simply

swipe the card in front of a reader. Within the last few years, that same technology has been introduced to credit cards and U.S. passports, potentially putting holders at risk. It does not matter if the cards are kept in a wallet or a purse since they can transmit through them when prompted by a RFID reader, which are for sale on eBay. Using free software, hackers using a RFID reader can easily obtain account numbers and expiration dates simply by placing the reader within a few inches of the card. The only credit cards that are vulnerable are those that allow users to tap or pass a reader to pay rather than swiping. Some might also have a symbol on them that indicate they transmit.
Source: http://www.wfaa.com/home/Electronic-pick-pocketing-threatens-credit-cards-passports-72070657.html

11. *November 23, DarkReading* – (International) **Employees willing to steal data; companies on the alert.** Employees know it is illegal to steal company data, but they are prepared to do it anyway. Companies know their employees are a chief threat to their data, but most are not doing much about it. These are the takeaways from two separate studies published today by security vendors Cyber-Ark and Actimize. Taken together, the studies paint a sobering picture of the state of trust and security within the corporate walls. In its study, Cyber-Ark surveyed some 600 workers in the financial districts of New York and London and found that most workers are not shy about taking work home — and keeping it for their own use. Eighty-five percent of the respondents to the Cyber-Ark survey said they know it is illegal to download company data for personal use, but 41 percent said they already have taken sensitive data with them to a new position. About a third of respondents said they would share sensitive information with friends or family in order to help them land a job. Almost half of the respondents (48 percent) admitted if they were fired tomorrow they would take company information with them, Cyber-Ark says. Thirty-nine percent of people would download company/competitive information if they got wind that their job were at risk. A quarter of workers said the recession has made them feel less loyal toward their employers. Of those who plan to take competitive or sensitive corporate data, 64 percent said they would do so “just in case” the data might prove useful or advantageous in the future. Twenty-seven percent said they would use the data to negotiate their new position, while 20 percent plan to use it as a tool in their new job. Customer and contact lists were the top priority for employees to steal, registering 29 percent of the respondents. Plans and proposals were next (18 percent), with product information bringing up the rear (11 percent). Thirteen percent of savvy thieves said they would take access and password codes so they could get into the network once they have left the company and continue downloading information and accessing data.
Source: http://www.darkreading.com/insiderthreat/security/management/showArticle.jhtml?articleID=221900815

[Return to top]

Transportation Sector

12. *November 24, Washington Examiner and Assocaited Press* – (Maryland) **Route 90 Bridge to reopen Tuesday.** The Maryland State Highway Administration says the Route 90 Bridge into Ocean City will reopen earlier than expected. The SHA says the Ocean City Expressway Bridge over the Assawoman Bay in Worcester County will reopen at 10 a.m. Tuesday. It had been scheduled to reopen in the middle of next month. The 38-year-old bridge closed October 15 after inspectors found deterioration in a girder requiring immediate attention. Traffic was detoured to the US 50/Harry Kelly Bridge. Workers removed the damaged bridge span, replaced steel girders, poured a new concrete deck and installed new raised pavement markings and stripes.
Source: http://www.washingtonexaminer.com/local/ap/route-90-bridge-to-reopen-tuesday-71867397.html

13. *November 24, Aero-News Network* – (Nevada) **Nevada airport waiting to re-open.** Carson City, Nevada is ready to open its newly-constructed eastern runway, and is only waiting for the completion of an FAA survey before putting the airport back in use. The airport closed November 9th for the runway construction, which Carson City officials said was the city's biggest stimulus project at $9.6 million. The runway was realigned three degrees to the north, and since the FAA went to a new surveying system, every new runway needs to be surveyed. The Nevada Appeal reports that the project included removing an 80-foot-high hill at one end of the runway. The airport will also build taxiways, install weather reporting gear and taxiway lights. Work is continuing on the western section of the airport, which is expected to be completed by December. The airport remained open as much as possible during the construction, but had to be completely closed earlier this month. Now, delays in the FAA survey are making airport tenants antsy. "It's very frustrating for us after we've gone through this phasing, but eventually, it falls out of our control. We're in contact with them every day, a few times every day, and all our users and tenants are very anxious," said an airport manager. The new runway will make it possible for larger business jets and more charter flights to use the airport.
Source: http://www.aero-news.net/index.cfm?ContentBlockID=cb7f685d-7209-4291-ae51-7cbb75ed388e

14. *November 24, Salisbury Daily Times* – (Delaware) **Bridge collapses, forces road closure.** Commuters who use Old Furnace Road will need to find another route as a bridge collapse has forced the closure of the road for at least three months, officials said. According to the Delaware Department of Transportation, a set of structural pipes underneath the bridge between Cokesbury and Rementer roads gave way Wednesday, causing congestion on connecting arteries. A DelDOT spokesperson said the collapse was caused after the ground beneath the bridge was compromised by stormwater brought by recent heavy winds and rain. No vehicles were on the bridge at the time of the collapse, she said. "Because of the high level of traffic that goes through that area, we have determined it to need emergency repairs," she said. By declaring it an emergency, she said the state can bypass a number of permitting processes. The state has not yet estimated the cost of the project. DelDOT's engineers review all state bridges annually. The spokeswoman said no problems were found during the most

recent inspection conducted in July.
Source: http://www.delmarvanow.com/article/20091124/DW01/911240305

15. *November 24, Wall Street Journal* – (National) **FAA plans tougher ice rules.** Federal aviation regulators on Monday proposed requiring enhanced ice-protection systems on hundreds of small turboprop aircraft, a step long advocated by government crash investigators and other safety experts. Capping government-industry debates and safety assessments originally sparked by fatal crashes stretching back to the 1990s, the Federal Aviation Administration envisions retrofitting many of the planes with onboard equipment that would automatically activate to shed ice before it can accumulate to dangerous levels on critical surfaces. Other turboprop models that would be affected by the proposed rule would be mandated to install new ice-detection equipment or use other methods to provide pilots clear-cut warnings that they must turn on deicing devices or change flight paths to prevent such accumulation. The agency also said it will consider whether many more aircraft — including some larger, widely used turboprops — should be subject to the same tougher standards. Smaller planes typically have less-advanced ice-detection and deicing systems than larger ones, and an FAA study found that major icing accidents over the years tended to occur almost entirely with small turboprops. But reflecting continuing controversy over icing dangers, the FAA document disclosed that the regulator is still studying recommendations from an advisory group about which current models shouldn't be permitted to fly at all in known icing conditions. The proposal specifically responds to a two-year-old recommendation from the National Transportation Safety Board stemming from a Cessna Citation jet that crashed in 2005, killing eight people. Though the plane was flying through icing conditions, the pilots failed to activate their ice-protection system. Larger aircraft, such as regional jets, typically already have more-advanced, automatic ice-protection devices. Since the summer, new commercial-aircraft designs across the board have been required to include enhanced ice protections.
Source:
http://online.wsj.com/article/SB125899048336560585.html?mod=googlenews_wsj

16. *November 23, eWeek* – (National) **FAA issues post-mortem report on flight-plan system failure.** The culprit of the FAA 4-hour flight-plan system failure was eventually determined to be a routing error in the software configuration inside a telecom router link at the FAA's Salt Lake City data distribution hub, pushing the router offline. The Federal Aviation Administration's national flight-plan filing system went down for 4 hours on the morning of Nov. 19, disrupting the takeoffs of hundreds of commercial flights and throwing hundreds of thousands of travelers off schedule. The faulty router, which for reasons not yet established was not able to default to a backup, also shut down a second major system node in Hampton, Georgia, effectively bringing to a halt the inputting of flight plans filed by U.S. commercial pilots. Commercial aircraft cannot take off from a U.S. airport without filing a flight plan.
Source: http://www.eweek.com/c/a/Enterprise-Networking/FAA-Issues-PostMortem-Report-on-FlightPlan-System-Failure-260111/

For another story, see item **2**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

17. *November 23, Associated Press* – (North Carolina) **NC Slim Jim plant explosion claims 4th victim.** A fourth victim has died from injuries suffered in a natural gas explosion that tore through a North Carolina Slim Jim plant five months ago, a hospital spokesman said Monday. The man died Thursday at the North Carolina Jaycee Burn Center in Chapel Hill, a spokesman said. Four critically burned victims were among the 71 who required hospital treatment after the June blast at the ConAgra Foods Inc. plant in Garner, said a U.S. Chemical Safety Board lead investigator. More than 200 people were working in the plant when the explosion in the packaging area caused part of the roof to collapse. Three others killed as a result of the explosion were struck by debris or crushed when part of the building collapsed. The man worked for Energy Systems Analysts Inc., a Hickory company hired to install a water heater. Two federal agencies have blamed natural gas for the blast. The Chemical Safety Board said contractors installing the water heater likely vented natural gas inside the building before the explosion as they purged a gas line. Officials said the gas should be vented outside. ConAgra resumed diminished production at its Garner plant in July after paying plant workers' wages for more than a month after the blast. The company said in September it would lay off about 300 of the factory's 750 remaining workers. Federal officials expect the full investigation of the ConAgra plant blast to be finished in 2010. Source: http://abcnews.go.com/Business/wireStory?id=9157934

[Return to top]

Water Sector

18. *November 24, San Francisco Examiner* – (California) **Half of the city in danger of losing water.** Water officials are rushing to repair a massive pipe to ensure the eastern half of San Francisco continues to have clean water. With one of the two pipes that carry drinking water into an out-of-service reservoir, the San Francisco Public Utilities Commission, which handles water distribution, is rushing to make the repairs, lest anything damage the second pipe. Joints between steel pipes laid in recent decades inside a tunnel 40 feet underground were found to be corroded late last month after leaking water flooded Tioga Avenue in the Visitacion Valley neighborhood. The corroded, 36-inch pipe, called Crystal Springs 1, is one of two built to carry Hetch Hetchy Valley snowmelt north from the Crystal Springs Reservoir on the Peninsula into the University Mound Reservoir in San Francisco. The water is then stored and

distributed to the eastern half of the city, including downtown. All the water that had been carried by the pipe is now being fed through Crystal Springs 2, a 60-inch pipe that runs roughly parallel to the older pipe. It is not known when Crystal Springs 1 began leaking, but 2,200 feet of piping was shut down after the leaks were detected last month, preventing any water from flowing through. If Crystal Springs 2 fails because of old age or due to an earthquake before Crystal Springs 1 is repaired, the University Mound Reservoir could run dry within two days, according to the Public Utilities Commission water manager. The reservoir is one of two major ones in the city. If such a scenario unfolds, utility workers would have to frantically attempt to reroute the water network to continue providing water for eastern and downtown San Francisco. "If [Crystal Springs] 2 went out for some reason, we would really be hard-pressed to deliver water," the water manager said. "Our plumbers would have to work miracles." The Public Utilities Commission is not equipped to repair the corroded pipe, agency documents show. Repair work by A. Ruiz Construction is expected to last until the end of December, agency documents show.
Source: http://www.sfexaminer.com/local/Half-of-The-City-in-danger-of-losing-water-72191267.html

19. *November 23, Oregonian* – (Oregon) **State investigates Oregon City sewage spill.** Environmental authorities are investigating whether an Oregon City treatment plant that dumped 2.54 million gallons of untreated sewage into the Willamette River violates state licensing standards. The Tri-City Water Pollution Control Plant lost power for six hours Sunday as a result of high winds, producing one of the larger raw-sewage spills in recent years, state environmental experts said Monday. "They are required to have at least two separate power feeds into the plant so if one goes down, they have a back-up," said a natural resource specialist with the state Department of Environmental Quality. "Typically, you don't have power outages across multiple grids, which raises the possibility that they could have been on the same circuit." The plant could face substantial fines if investigators determine that the power sources were not properly separated. Investigators said they may not know for several days whether both the plant's primary and back-up power sources were drawing from the same feeder line. An initial examination by PGE Monday indicated that an overhead line may have fallen in exactly the right place to take out the two separate lines running to the plant. A fuller "root-cause" evaluation will be undertaken later to determine if that's what happened, said a PGE spokeswoman. Plant personnel reported the power outage at 11:20 a.m. Sunday. Portland General Electric crews restored service at 5:22 p.m. With the pumps shut down, raw sewage from the plant's six-city service area had nowhere to go but into the river. The plant currently is undergoing expansion, in part to help treat sewage diverted from the Kellogg Creek plant in Milwaukie, which is near capacity. As part of the expansion, an emergency generator is being installed.
Source: http://www.oregonlive.com/clackamascounty/index.ssf/2009/11/state_investigates_oregon_city.html

20. *November 23, Water Technology Online* – (National) **Failing sewer systems overwhelm waterways.** In the last three years, nearly 40 percent of the nation's

sewage systems — including those in major cities like New York — have reported violating federal clean water laws by releasing untreated or partially treated human and industrial waste into waterways, according to the latest of The New York Times series of articles on the state of America's waters and regulators' responses. In the report, "As Sewers Fill, Waste Poisons Waterways," the reporter examines data that reveals how outdated combined sewer/stormwater treatment systems fail, especially during heavy rainstorms, creating overflow discharges into the environment as well as violations of the Clean Water Act of 1972. He reports: "Fewer than one in five sewage systems that broke the law were ever fined or otherwise sanctioned by state or federal regulators, the Times analysis shows. It is not clear whether the sewage systems that have not reported such dumping are doing any better, because data on overflows and spillage are often incomplete." The report also examines how untreated sewage ends up in drinking water sources, and how academic research suggests that as many as 20 million people each year become ill from drinking water containing bacteria and other pathogens that are often spread by untreated waste.
Source: http://watertechonline.com/news.asp?N_ID=72997

[Return to top]

Public Health and Healthcare Sector

21. *November 24, Associated Press* – (Ohio) **VA spokeswoman confirms investigation of alleged snooping into records of Ohio bodies suspect.** The Veterans Affairs hospital in Cleveland says it is looking into whether employees nosed around in the private medical records of a suspected serial killer. Stokes Cleveland VA Medical Center's spokeswoman tells the Plain Dealer newspaper she cannot say anything more than to confirm an investigation into the alleged snooping is under way.
Source: http://www.fox8.com/news/sns-ap-us--cleveland-bodiesfound-varecords,0,6304658.story

22. *November 24, Associated Press* – (International) **Swine Flu RECALL: H1N1 vaccine pulled in Canada.** Pharmaceuticals company, GlaxoSmithKline PLC, said Tuesday it has advised medical staff in Canada to not use one batch of swine flu vaccines in case they trigger life-threatening allergies. A company spokeswoman said that they issued the advice after reports that one batch of the swine flu vaccine might have caused more allergic reactions than normal. "We have advised health care professionals not to use that batch while health authorities and GlaxoSmithKline investigate," she said. She said the batch at issue, which has been distributed across Canada, contains 172,000 doses of the vaccine. She declined to say how many doses had been administered before the advice to stop using them was given.
Source: http://www.huffingtonpost.com/2009/11/24/swine-flu-recall-h1n1-vac_n_368776.html

23. *November 24, Chattanooga Times Free Press* – (Tennessee) **BlueCross offers credit monitoring after Social Security numbers compromised.** After 68 computer hard drives were stolen last month, BlueCross BlueShield of Tennessee is providing

members whose Social Security numbers may be at risk with credit monitoring service for a year. On October 2, someone entered a data closet at the insurance provider's Eastgate Town Center location and removed hard drives containing encoded data. BlueCross is assisting the criminal investigation and will retain an independent firm to perform a security assessment, the company said in a news release Monday. More than 800 staff members, a temporary staffing service and a data security contractor are working six days a week to retrieve and review back-up files, the release stated. Chattanooga police continue to pursue leads in the case, hoping the hard drives will show up when someone attempts to sell or discard them.
Source: http://www.timesfreepress.com/news/2009/nov/24/bluecross-offers-credit-monitoring-after-social/

[Return to top]

Government Facilities Sector

24. *November 23, U.S. Department of Justice* – (International) **Arms dealer pleads guilty to conspiracy to supply U.S. fighter jet engines to Iran.** A Belgian national and resident of France suspected of international arms dealing for decades, pleaded guilty today in U.S. District Court for the Southern District of Alabama to conspiracy to illegally export F-5 fighter jet engines and parts from the Untied States to Iran. The defendant, along with his co-conspirator, an Iranian national currently living in France, was charged in a six-count indictment returned on August 27, 2009, with conspiracy, money laundering, smuggling, as well as violations of the Arms Export Control Act and the International Emergency Economic Powers Act. The defendant was arrested by federal agents in August 2009 upon his arrival in New York. The co-conspirator remains at large. According to the defendant's factual proffer and the documents filed in court, he, along with his co-conspirator, are experienced arms dealers who have been actively working with the Iranian government to procure military items for the Iranian government. In February 2009, the defendant contacted an undercover agent seeking engines for the F-5 (EIF) fighter jet and the C-130 military transport aircraft for export to Iran. Thereafter, the defendant began having regular e-mail contact with the undercover agent regarding the requested F-5 engines and parts.
Source: http://www.justice.gov/opa/pr/2009/November/09-ag-1272.html

[Return to top]

Emergency Services Sector

25. *November 24, The Mercury News* – (Pennsylvania) **Montco emergency call info available in real time.** Montgomery County Department of Public Safety rolled out an online site Monday morning where Internet users can view emergency service calls for fires, traffic accidents and medical emergencies. The deputy director of Public Safety Communications and Technology told reporters during a conference call that the new Web site will upload incidents in near real-time 24 hours a day, though not all calls would be posted. "It has a five-minute delay," he said. "It will give locations and

details, but there are no police-related incidents." Omitting police calls is meant to ensure officers' safety. The emergency officials also said no residential address would be published online, "only the existence of a (street) block," he said. And the names of medical or psychiatric patients being treated or transported by ambulance would not be made public. The Internet site, http://dps.montcopa.org/webcad, also has special pages for Web-enabled mobile phones, as well as links to live audio streams of actual fires and medical radio channels.
Source:
http://www.pottstownmercury.com/articles/2009/11/24/news/srv0000006908540.txt

26. *November 23, The Times and Democrat* – (South Carolina) **Drill allows emergency personnel to test response.** The scene at F.R. Huff Drive at the old Hamricks building in St. Matthews Saturday morning was grim. A school bus was lying on its side, and injured people were everywhere. Fortunately, the scene was part of a surprise, full-scale emergency disaster drill involving Calhoun County Emergency Services personnel. The scenario had a propane gas truck colliding with a school bus, which overturned in the collision. The simulation included two school bus occupants and the propane gas truck driver being killed and numerous individuals injured inside and outside of the bus. The Calhoun County Emergency Services operations manager said agencies participating in the drill were Calhoun County EMS, the St. Matthews Volunteer Fire Department, the St. Matthews Police Department and the LifeNet South Carolina team from Orangeburg.
Source:
http://www.timesanddemocrat.com/articles/2009/11/23/news/doc4b0b25e859ad2236310793.txt

[Return to top]

Information Technology Sector

27. *November 24, IDG News Services* – (International) **Microsoft issues security advisory on IE vulnerability.** Microsoft on November 23 issued a security advisory that provides customers with guidance and workarounds for dealing with a zero-day exploit aimed at Internet Explorer. Earlier in the day, the company said it was investigating the incident which emerged over the weekend when someone published the exploit code to the Bugtraq mailing list. By Monday night, Microsoft switched gears and issued the advisory. There have not been any active exploits of the vulnerability reported so far. Microsoft released Security Advisory 977981, which includes workarounds for an issue that exposes a flaw in Cascading Style Sheets that could allow for remote code execution. Vulnerabilities that allow remote-code execution generally result in patches rated as critical by Microsoft. The advisory confirmed the vulnerability affects IE 6 on Windows 2000 Service Pack 4, and IE 6 and IE 7 on supported editions of XP, Vista, Windows Server 2003 and Windows Server 2008. Microsoft's said users running IE 7 on Vista can configure the browser to run in Protected Mode to limit the impact of the vulnerability. It also recommended setting the Internet zone security setting to "High" to protect against the exploit. The "High" setting will disable JavaScript, which

currently is the only confirmed attack mode. Microsoft said IE 5.01 Service Pack 4 and IE 8 on all supported versions of Windows are not affected. For an attack to work, the hacker would first have to get his victim to visit a Web site that hosted the exploit code. This could be a malicious Web site set up by the hacker himself or it could be a site that allows users to upload content. Another way cyber criminals have launched this type of attack, however, is by hacking into legitimate Web sites. Earlier this week, for example citizen's band radio vendor Cobra Electronics disclosed that it had been hacked in June, most likely by a professional hacker who had used the site to download malware to customers.
Source:
http://www.computerworld.com/s/article/9141378/Microsoft_issues_security_advisory_on_IE_vulnerability

28. *November 23, The Register* – (International) **IE bug leaks private details from 50m PDF files.** A bug in Microsoft's Internet Explorer browser is causing more than 50 million files stored online to leak potentially sensitive information that could compromise user privacy, a security researcher said. The documents stored in Adobe's PDF format display the internal disk location where the file is stored, an oversight that can inadvertently expose real-world names and login IDs of users, the operating system being used and other information that is better kept private. The data can then be retrieved using simple web searches. Google searches such as this one expose almost four million documents residing on users' C drives alone. Combined with searches for other common drives, the technique exposes more than 50 million files that display the local disk path, according to Inferno, a security researcher for a large software company who asked that his real name not be used. "If they have those kind of PDFs, somebody can use search engines to find out user names or do more reconnaissance on the operating systems used," he told The Register. "That actually invades the privacy of a user." The potentially sensitive data is included in PDFs that have been printed using Internet Explorer. The full path location is appended to its contents as soon as the Microsoft browser is used to print the document. Although the data isn't always exposed when the document is viewed with Adobe Reader, it is easily readable when the file is opened in editors such as Notepad, and the text is also available to Google and other search engines. This PDF, for example, was stored at C:\Program Files\Wids7\WizardReport.htm at time of printing. The path makes it clear that the file was stored on a Windows machine that has software from Worldwide Instructional Design System installed. Other PDFs give up directory names that reveal authors, projects or other data that may have been designated confidential. The only way to remove the path is erase the text in an editor and save the document.
Source:
http://www.theregister.co.uk/2009/11/23/internet_explorer_file_disclosure_bug/

29. *November 23, The Register* – (International) **Google hoodwinked into pushing Chrome OS scareware.** Rogue anti-virus scammers have tainted search results for Chromium OS - the open source version of Google's Chrome OS - in a bid to expose surfers hunting the web operating system to a fake anti-virus scan scam instead. Search terms such as "chromium os download" point to sites featuring scripts that redirect

stray surfers towards scareware scam portals. These sites falsely report that users PCs are loaded with malware before pushing users to download a clean-up tool little or no utility. The SecureKeeper utility offered through the scam uses a series of aggressive and misleading tricks to coerce people into paying $49.95 to purchase a licence, as explained in a blog post by security firm eSoft here. Something very similar happened when Google released its Wave collaboration tool. In both cases, surfers are only redirected to scareware-punting portals in cases where they arrive as bobby-trapped URLs via Google search results. Both the Google Wave and Chromium Os scams refer to a product or service that is not yet generally available, a factor that arguably increases the potency of scams. Both attacks (like many before them) rely on black hat Search Engine Optimisation techniques. Cybercrooks typically break into well-established sites and create webpages stuffed full with relevant keywords, cross-linked to other sites doctored using the same technique. The tactic is geared towards tricking search engines into pushing manipulated URLs higher up the search engine indexes for targeted terms.
Source: http://www.theregister.co.uk/2009/11/23/chromium_scareware/

30. *November 23, Wall Street Journal* – (International) **EarthLink says email service restored.** EarthLink on Monday blamed a server migration for the outages that disrupted email service for its customers over the weekend but said the problem has been solved. Many EarthLink subscribers lost email access over the weekend due to a server migration. “Some EarthLink email customers experienced a delay in receiving emails over the weekend. This issue was associated with EarthLink’s migration of our MindSpring customers to a new EarthLink email server,” a spokeswoman for the Atlanta Internet-services providers said in a statement. “EarthLink has corrected the problem and we believe all delayed emails have been delivered to our customers.”
Source: http://blogs.wsj.com/digits/2009/11/23/earthlink-says-email-service-restored/

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

31. *November 24, McClatchy* – (Texas) **TWTC fire in Dallas blamed for Sunday Internet out.** A short-circuit and fire in Dallas is being blamed for a broadband outage Sunday night that left 7,314 Windstream customers in Kerrville and the surrounding Hill Country without Internet access for about 12 hours. A division vice president for Windstream, a telecommunications company providing Internet and telephone service, said the problem was with equipment for Time Warner Telecom. In order to provide broadband service to Kerrville, Windstream uses data transport lines operated by Time

Warner Telecom that connect to a central hub in Dallas. He said he was informed by Time Warner Telecom that a short-circuit in the Time Warner Telecom equipment caused a "localized fire," which caused an outage from around 3:50 p.m. Sunday until 4:10 a.m. Monday. The outage affected customers from Kerrville to the Harper area
Source: http://www.tradingmarkets.com/.site/news/Stock News/2676502/

For more stories, see items **16** and **30**

[Return to top]

Commercial Facilities Sector

32. *November 23, KTXL 40 Sacramento* – (California) **Arden Mall Macy's evacuated following threat.** Customers were briefly evacuated from the Macy's Department Store anchoring one side of Arden Fair Mall Monday morning. Sacramento Police responded to reports of a bomb threat delivered to the store sometime shortly after 10:00am Monday. Customers were evacuated as a precaution. Shoppers were allowed to return to stores around 10:40am. Police are investigating the circumstances of the bomb threat.
Source: http://www.fox40.com/news/headlines/ktxl-news-macysevac1123,0,3009123.story

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

33. *November 23, Houma Today* – (Louisiana) **Officials: Trucks damaging levee in Terrebonne.** Trucks hauling dirt to build a subdivision are damaging a levee that protects the Barrios neighborhood from flooding, Terrebonne Parish, Louisiana officials and neighbors say. But owners who are developing their land say the levee has been compacting, or sinking, for years and that their construction trucks are not a cause. The property and levee are the future home of a commercial-and-residential subdivision that would include an L-shaped boat slip, a water feature many neighbors contend will increase flood risks to their homes in Barrios, Mulberry, and Lamar. The slip, up to 150 feet wide and more than nine football fields long, would be dug off the Gulf Intracoastal Waterway. The property's levee extends west from the end of Concord Road parallel to the Gulf Intracoastal Waterway. Under the parish's right-of-way agreement, the property owner can use the levee to access the land, officials said. The agreement also says the owners cannot damage the levee or interfere with the parish's maintenance of it. In some spots, the levee has compacted, or sunk, 1-5 inches since the

last survey in 2005, according to the parish's survey taken Thursday. "There are some minor variances from our target elevation of 6.5 (feet)," said the Parish manager. "We believe it's due to the hauling of dirt." The parish has not ordered the trucks to stop using the road, he said. Instead, the parish has asked the owners and their engineers to come up with a plan to address the levee's height, but as of Friday no proposal was offered. If the owners fail to repair the damage, the parish can either make the repairs and bill them or take them to court.
Source:
http://www.houmatoday.com/article/20091123/ARTICLES/911239944/1026?tc=autorefresh

[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 Website: 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