Homeland Security

Daily Open Source Infrastructure Report for 3 December 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- According to Reuters, the failure of a river water supply line and flooding at the Susquehanna nuclear power station in Columbia County, Pennsylvania forced owner PPL Corp to reduce power to one reactor on Tuesday. (See item **5**)
- Bloomberg reports that air passengers may be at risk of terrorist attacks because of air-cargo screening flaws, according to a report released by the Homeland Security Department's inspector general on Monday. Thirty percent of 6,767 cargo inspections by the Transportation Security Administration found security violations in the three quarters ended in June 2008. (See item **21**)

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. *December 1, Sharon Herald* – (Pennsylvania) **AG: Gas pipeline leak fouls well site.** A Cortland, Ohio company operating a natural gas pipeline in West Salem Township has been charged by the Pennsylvania Attorney General's (AG) office with illegally discharging oil and other waste in the township. Energy Exploration & Development

LLC, formerly known as Energy Exploration Inc., was charged November 16 with unlawful conduct for allegedly dumping oil and brine, or salt, water from a section of pipeline along state Route 358, according to a news release issued on December 1. Between July 11 and August 13, oil and brine water stained a 30-foot area of soil and vegetation near an abandoned gas well site. The waste was contained to a "relatively small area," the AG deputy press secretary said. The company had no permit from the Department of Environmental Protection (DEP) to dump waste in that location. DEP in July 2008 and July 2009 sent the company violation notices that they failed to install measures that would prevent pollution. DEP told the company to replace a plastic tank at the end of the pipeline with a metal one, but they failed to follow orders, and the pollution and criminal charges could have been prevented. The company is charged with violating Pennsylvania's Oil and Gas Act and Solid Waste Management Act for dumping waste without a DEP permit, a third-degree misdemeanor that carries a fine of $1,000 to $2,500 a day. They are also charged with failing to properly maintain a natural gas pipeline, an ungraded misdemeanor with a fine of up to $5,000.
Source: http://www.sharonherald.com/local/local_story_335223213.html

2. *December 1, Bradenton Herald* – (Florida) **Copper wire thefts at east county utility.** Peace River Electric Cooperative officials reported on November 30 three more incidents of copper wire being stolen from their utility poles. According to a Manatee County Sheriff's Office report, between 28,000-32,000 feet of copper wiring was stripped from the poles, but because the thieves took only the neutral wire there was no disruption of electrical service. The value of the wire was $8,000-$9,000, according to the report. The wiring was taken from three stations at Taylor Road and Singletary Road, 14805 Sugar Bowl Road, and 8900 Bunker Hill Road. "Copper thefts have been up just recently," said a spokesman for the sheriff's office. "Maybe in the last six weeks we've seen it more." He said copper thefts were more broad-base a couple of years ago with copper plumbing and electrical wiring targeted when the price per pound was higher, but the recent thefts seem to be only targeting the utility companies.
Source: http://www.istockanalyst.com/article/viewiStockNews/articleid/3675642

For another story, see item **30**

[Return to top]

Chemical Industry Sector

3. *December 2, Delaware Gazette* – (Ohio) **Chemical spill near freeway contained.** Firefighters and hazmat crews with multiple fire departments from throughout Delaware County, Ohio, responded to a hazardous chemical spill at an area truck stop Tuesday morning. More than 300 gallons of what was thought to be potassium hydroxide, an acidic chemical, were spilled around 11 a.m. Tuesday by a semi truck at the Pilot Travel Center on U.S. 36/Ohio 37, officials said. Initially thought to be a small leak, upon further investigation it was determined to be a more significant leak, prompting a larger response from area fire departments.
Source: http://www.delgazette.com/local.asp?ID=1887&Story=2

4. *December 1, Connecticut Post* – (Connecticut) **Blaze hits chemical warehouse in Fairfield.** Fire struck a chemical warehouse off the Post Road in the Southport section of Fairfield, Connecticut, early November 26, requiring an hours-long hazardous materials cleanup at the business. No one was hurt, despite heavy flames that erupted shortly before 2 a.m. in a storage warehouse at Superior Plating Co., 1480 Post Road, corner of Lacey Place, and officials said initial tests show there was no significant environmental impact from the fire. Firefighters poured large amounts of water on the fire for about two hours to neutralize the chemicals. Two drums contained chemicals used to treat ground water. Once hit with water, the chemicals began decomposing and generating heat, which then began melting the metal drums. The cause of the fire has not yet been determined.
   Source: http://www.connpost.com/ci_13901694

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *December 2, Reuters* – (Pennsylvania) **Susquehanna 3rd reactor in Pa to report incident.** The failure of a river water supply line and flooding at the Susquehanna nuclear power station in Pennsylvania forced owner PPL Corp to reduce power to one reactor on Tuesday, the company told the U.S. Nuclear Regulatory Commission. Power at the 1,140-megawatt Unit 2 was lowered to 79 percent, from about 94 percent. A plant spokesman could not say when the plant would return to full power due to competitive reasons. The company was still assessing the problem at the plant, located in Berwick in Columbia County. The incident involved the failure of the supply line bringing river water to the Unit 2 cooling tower, causing the valve vault to flood and overflow at several thousands of gallons per minute. The vault is about 12 feet deep and 12 feet across. The plant was still pumping water from the river to the vault and then pumping the water from the vault to the cooling tower, the spokesman said. PPL called the local fire company to provide equipment to help pump out the vault. The river water overflowing the vault entered nearby storm drains and a nearby building housing nonsafety-related equipment. The water entering the sewer did not constitute a reportable spill. The company reduced Unit 2 to minimize the impact to the cooling tower. The failure of the supply line had an insignificant impact to the environment because radiological levels were less than lower-limit detection, but noted the flooding was likely to cause heightened public and government concern, the company said.
   Source:
   http://www.reuters.com/article/companyNews/idUSN0254897320091202?pageNumber=1&virtualBrandChannel=0

6. *December 2, TCPalm.Com* – (Florida) **St. Lucie Nuclear Power Plant to test sirens on Thursday.** The St. Lucie County Department of Public Safety and the Martin County Department of Emergency Services will conduct a quarterly test of the outdoor warning sirens for Florida Power & Light's St. Lucie Nuclear Power Plant at noon on Thursday, December 3. The test will involve a one-minute sounding of all 90 sirens within the 10-mile St. Lucie Emergency Planning Zone. Before and after the sirens

sound, a message will be broadcast on the sirens public address system stating: "This is only a test." There will be a 15-second wail of the sirens at the end of the final test announcement. The testing of the siren system is to improve public awareness of its function and ensure it is in operable condition. In the unlikely event of an actual emergency at the St. Lucie Nuclear Power Plant, the sirens would sound for a five-minute period, followed by official instructions and another five-minute sounding of the siren system. Detailed instructions for the general population would be then broadcast over local radio and television.
Source: http://www.tcpalm.com/news/2009/dec/02/st-lucie-nuclear-power-plant-test-sirens-thursday/

[Return to top]

Critical Manufacturing Sector

7. *December 2, Detroit News* – (National) **Stricter side air bag rules proposed.** The National Highway Traffic Safety Administration (NHTSA) on Tuesday proposed new rules that would require automakers to make larger and stronger side air bags to prevent motorists from being thrown out of vehicles during rollover crashes. The plan would set new performance standards for "ejection mitigation" and is aimed at reducing the roughly 10,400 deaths in rollover crashes every year. NHTSA said the new rule, when completely implemented, would save 402 lives and 302 serious injuries annually. Most of the benefit would be for motorists not wearing seat belts, but NHTSA estimates that 13 percent of those wearing seat belts also would benefit. NHTSA estimates the cost at $54 per vehicle, or $920 million annually. The new rules would apply to vehicles 10,000 pounds or less and would likely require "side curtain air bags to be made larger to cover more of the window opening, made more robust to remain inflated longer, enhanced to deploy in side impacts and in rollovers, and made not only to cushion but also made sufficiently strong to keep an occupant from being fully or partially ejected through a side window." NHTSA noted that Ford Motor Co. introduced its Safety Canopy side curtains in the 2002 model year that now inflate for six seconds, while General Motors Co.'s side curtain air bags remain open for five seconds. By contrast, side-impact or frontal air bags often stay open for just 0.1 second. NHTSA's proposed rule would tentatively apply to convertibles but not to walk-in vans. NHTSA has sought more information on whether police vehicles with security partitions should be covered. Twenty percent of a manufacturer's fleet would be required to comply by the 2014 model year, assuming it is finalized by August.
Source:
http://www.detnews.com/article/20091202/AUTO01/912020326/1148/auto01/Stricter-side-air-bag-rules-proposed

8. *December 1, Aviation Week* – (National) **787 first flight countdown resumes.** Boeing is preparing to reactivate the first 787 test aircraft for its long-delayed first flight later this month now that it has completed validation work on the modification to strengthen the side-of-body wing-fuselage join. Within hours of the announcement that static tests were finished late on November 30, the initial aircraft (ZA001) was rolled back out to

the Everett flight line. Flight test engineers appear to be wasting no time in getting ready to resume pre-flight work and plan to conduct several engine runs, including thrust reverser tests later this week. Work on the modification, which was required to beef up the wing join after tests earlier this year revealed weakness in the stringer caps, added a further six-month delay to the stalled development program. At the time of the new delay in June, the program was already running approximately 22 months behind schedule. However, Boeing says the '2C' loads verification tests on the static test airframe (ZY977), appears to have been positive and therefore sets the clock ticking toward the long-delayed first flight. The company expects "a full analysis of the test results to be concluded in approximately 10 days," but cautions that meeting the end of the month planned flight target depends on "a successful test result." The test subjected the 787 airframe, the wing and trailing edges to its limit load — the highest loads expected to be seen in service. "The load is about the same as 2.5 times the force of gravity for the wing," adds Boeing. The test verified the structural reinforcements made to the side-of-body section where new fittings were added at 34 stringer cap locations within the joint where the wing is attached to the fuselage. The modifications have been completed on the first two flight-test aircraft (ZA001 and ZA002,) as well as the full-scale static test aircraft (ZY997). Boeing plans to test the 787 wing to its ultimate load of 150 percent in around three to four months time, but is only required to exceed the 100 percent mark to enable flight tests to proceed.
Source:
http://www.aviationweek.com/aw/generic/story.jsp?id=news/FIRST120109.xml&headline=787 First Flight Countdown Resumes&channel=comm

For another story, see item **4**

[Return to top]

Defense Industrial Base Sector

9. *December 2, Aerospace Daily and Defense Report* – (International) **U.S. defense exports still dominate market.** China, France, and Russia are increasingly aggressive in courting customers for their military products, but it is the United States that is raking in the big dollars — and increasingly so. Additionally, the United States' improving relationship with India could signal that record high levels of military exports are not just an aberration but are sustainable. This prospect would bring relief to U.S. defense companies, which face the possibility of shrinking modernization projects when Washington starts focusing on cutting its massive budget deficit. A decade ago, the United States booked about $10 billion in foreign military sales (FMS). When those contracts reached $28 billion in fiscal 2008, many in the Pentagon thought it was an aberration, especially given the $10 billion jump from the year before. But there has been no sign of a letup. The director of the Defense Security Cooperation Agency says the value of FMS commitments signed during the last fiscal year reached $38.1 billion, and this year's total could top $50 billion based on estimates of deals in the negotiating pipeline.
Source:

http://www.aviationweek.com/aw/generic/story.jsp?id=news/EXPORT120209.xml&headline=U.S. Defense Exports Still Dominate Market&channel=defense

10. *December 1, Navy Times* – (Missouri) **Navy OKs increased production of Growler.** The Navy has approved full-rate production of the EA-18G Growler, the next-generation electronic attack aircraft that will begin replacing the EA-6B Prowlers on carrier decks next year. Boeing, which makes the Growlers, will ramp up production at its St. Louis plant to make about 20 aircraft per year to meet the Navy's target of 88 total electronic attack aircraft, Boeing officials said. The Navy's first Growler squadron, Electronic Attack Squadron 132, known as the Scorpions, has five aircraft and is based at Naval Air Station Whidbey Island, Washington. Navy officials expect it to deploy in 2010, but the carrier with which it will deploy remains unclear. The squadron is the first of 12 operational squadrons to stand up during the next three years. The Navy initially said the Prowlers would retire by 2012, but officials say they are now considering extending some aircraft for several years.
Source: http://www.navytimes.com/news/2009/12/navy_growler_120109w/

[Return to top]

Banking and Finance Sector

11. *December 2, Bloomberg* – (National) **U.S. SEC subpoenas more companies in insider probe, WSJ says.** The U.S. Securities and Exchange Commission sent at least 36 subpoenas to financial companies in a broadening investigation of potential insider-trading violations that includes Goldman Sachs Group Inc., the Wall Street Journal reported, citing unidentified people familiar with the matter. Some of the subpoenas are related to mergers in the health- care and retail industries over the past three years, including Sears Holdings Corp.'s failed attempt to buy Restoration Hardware in 2007, the newspaper said. The SEC has become more aggressive in enforcement, including insider-trading cases, since coming under new leadership this year, the newspaper said. The regulator has also come under scrutiny in Congress, where two senators have criticized its oversight of Pequot Capital Management Inc., once the world's biggest hedge-fund manager. Some of the subpoenas focus on investment bankers, including the role of Goldman bankers in about 12 health-care transactions since 2006, the people said, according to the report. Investigators also asked about other advisory firms, the people were cited as saying. The firms were not named in the report. In one of the subpoenas, the SEC asks hedge-fund managers and others about relationships and communications with Goldman bankers who worked on the health-care transactions, the people were cited as saying. It was not clear whether regulators had contacted Goldman in connection with the recent subpoenas or the nature of any contact, the newspaper said.
Source:
http://www.bloomberg.com/apps/news?pid=20601087&sid=a8WJjvtE0IjM&pos=6

12. *December 1, Emmetsburg News* – (Iowa) **Palo Alto area banks warn of new e-mail scam.** Financial institutions are warning their customers to be wary of a new e-mail

scam that's making the rounds during the busy holiday season. The scam recently came to light after many area residents reported receiving e-mails, purportedly from the Federal Deposit Insurance Corporation, or FDIC. The e-mail claims that the financial institution which the customer has opened an account with, is on a list of banks that are "failing" and that the FDIC is taking control of that institution's assets. The e-mail then instructs the recipient to click on a link that supposedly takes the recipient to the FDIC website, when in reality, the website is actually fake. When the recipient clicks on the fake FDIC website, they are prompted to enter sensitive information, such as account numbers for checking and savings accounts, and other personal information. Authorities report that the entire e-mail is completely bogus – nothing more than a "phishing" scam – one where criminals attempt to collect personal information from people that can be used to drain bank accounts without the owner's knowledge.
Source:
http://www.emmetsburgnews.com/page/content.detail/id/501981.html?nav=5001

13. *November 30, Associated Press* – (National) **After flooding economy, Fed to mop up money.** The Federal Reserve is fine-tuning a strategy to reel in some of the unprecedented amount of money that is been pumped into the economy during the financial crisis. The Federal Reserve Bank of New York said on December 1 that investors and others should not conclude anything about when the central bank will reverse course and start boosting interest rates and removing other supports to fend off inflation. The upcoming operations will involve so-called reverse repurchase agreements. That is when the Fed sells securities from its portfolio, with an agreement to buy them back later. Reverse repos are one tool the Fed can use to drain some money it has plowed into the economy to ease financial troubles. The operations will be "extremely small" and would not affect the Fed's key interest rate, officials said. They would not say what the amount for the operations would total. Fed officials also said they did not know when the first operation would be conducted and how many there would be. The operations will be conducted to "to ensure operational readiness" at the Federal Reserve, the New York Fed said. They do not "represent any change in the stance of monetary policy, and no inference should be drawn about the timing of any change in the stance of monetary policy in the future," the New York Fed said. The operations were designed to "have no material impact .... on market rates," the Fed added.
Source: http://www.msnbc.msn.com/id/34210280/ns/business-stocks_and_economy/

14. *January 1, Credit Union Times* – (Illinois) **ATM skimmers make off with $70,000 in Chicago.** In Chicago, police are confirming media accounts of two ATM thieves which made off with $70,000 from a bank ATM after they attached a device to the machine to record card data and used a camera to record a card holder's personal identification numbers as they punched them in. The bank declined to comment on the theft other than to confirm that the Secret Service had been notified as well as the police. The Secret Service did not comment. Media reports said the two were caught on surveillance cameras placing the device and then returning to collect it and use the data to make the withdrawals.

Source: http://www.cutimes.com/News/2009/12/Pages/ATM-Skimmers-Make-Off-With-70000-in-Chicago.aspx

[Return to top]

Transportation Sector

15. *December 2, Reuters* – (International) **Islamist rebels claim Russian rail bombing.** Islamist militants on Wednesday claimed responsibility for a bombing that derailed a Russian express train, killing 26 people, and vowed further "acts of sabotage" in a letter posted on a rebel website. Friday night's attack on the luxury Nevsky Express running between Moscow and St Petersburg was the worst in Russia outside the North Caucasus in five years and raised fears of a new wave of bombings in major cities. "This operation was prepared and carried out...pursuant to the orders of the Emir of the Caucasus Emirate Doku Umarov," the KavkazCenter.com website said, quoting a letter it said it received from Islamist rebels. A second, smaller bomb detonated by mobile phone injured Russia's top detective as he visited the crime scene on Saturday. The Investigative Committee said its chief was hospitalised as a result of the blast but would not comment on his condition. The militants' letter said the train bombing was part of a campaign of sabotage against strategic economic targets. "These acts of sabotage will continue for as long as those occupying the Caucasus do not stop their policy of killing ordinary Muslims," the letter said. On Monday, another bomb exploded under a train en route from Siberia to Azerbaijan in Russia's troubled Dagestan region, but there were no deaths.
Source: http://www.reuters.com/article/homepageCrisis/idUSGEE5B108E._CH_.2400

16. *December 2, WJLA 7 Washington, D.C.* – (District of Columbia) **Metro's Oversight Committee to conduct first track inspection.** Independent safety monitors with the Tri-State Oversight Committee are scheduled to inspect Metro tracks for the first time Wednesday. The Committee Chairman told the Washington Post that the group scheduled several days of inspections for December. This comes after months of controversy surrounding the Washington Post report that Metro barred independent monitors from live tracks for inspections. Then, in a sudden change of heart, Metro decided to lifted its long-standing ban and grant independent safety monitors access to the tracks. Since the spring, monitors, from the Tri-State Oversight Committee, have pressed Metro via e-mails and in person for access to determine whether the transit agency was following proper safety guidelines after several Metro employees were fatally injured on the tracks. But Metro declined the monitors' several attempts, the Post report found. Two Metro employees were both killed on the job while the independent monitors sought access to the tracks.
Source: http://www.wjla.com/news/stories/1209/683438.html

17. *December 2, Associated Press* – (New York) **NY report faults subway emergency planning.** A state inspector general says New York City's transit agency should designate someone to oversee emergency planning for the subways. A Metropolitan Transportation Authority (MTA) report says transit officials failed to establish clear

procedures for employees who coordinate with other agencies during emergencies. The transit agency has since clarified its procedures. The report says such shortcomings could have left riders at risk during fires, crimes and other emergencies. NYC Transit says riders' safety was never compromised. The New York Times obtained a copy of the report, which is being released this week. The Inspector General also tells the Times that staff memos are not an adequate training method. The MTA is the parent agency of NYC Transit.
Source: http://www.wcax.com/Global/story.asp?S=11604665

18. *December 2, Associated Press* – (Mississippi) **High tech cameras going up along Miss. River, Vicksburg port sites.** A $444,988 federal grant will provide for installation of high-resolution surveillance cameras at Mississippi River and port sites in Vicksburg and Warren County. City officials tell the Vicksburg Post that initial plans call for a dozen cameras to be placed at points along the river and at the Port of Vicksburg to watch river traffic and identify potential threats. The cameras may be monitored at the Vicksburg Warren E-911 Dispatch Center. The Department of Homeland Security funds will cover two-thirds of the cost, with the remainder coming from in-kind donations, which can include site donations. Cameras are already in place at the river bridges and some port locations.
Source: http://www.wreg.com/news/sns-ap-ms--rivercameras,0,1189.story

19. *December 1, KCNC 4 Denver* – (Colorado) **Denver Police Department division chief eyed in Denver International Airport security breach.** BS4 has learned that the Transportation Security Administration (TSA) is investigating a top-ranked Denver police officer suspected of breaching security at Denver International Airport (DIA). It is unclear where the division chief was headed. A Denver police lieutenant told a CBS4 investigator "the TSA is involved and their investigation is independent of ours." A TSA spokesperson told CBS4 she could not comment or provide any information on the case or any specific security breaches. But numerous other sources confirmed the TSA investigation, one saying TSA had issued a "letter of investigation." Other sources said TSA investigators were gathering statements from Denver police officers at DIA who may have information about the security breach. Several sources familiar with the incident and the investigation provided the following account: During a security audit, TSA investigators discovered that the division chief had recently used a special electronic access card that allowed him to bypass TSA security screeners at DIA and gain access to airport concourses and board a plane. Those cards are only supposed to be used for law enforcement officers and other personnel on official airport business.
Source: http://cbs4denver.com/investigates/tsa.dia.security.2.1344084.html

20. *December 1, Associated Press* – (Florida) **Cops: Woman makes threat to help boss make flight.** A South Florida woman has been charged with calling in a bomb threat to keep her boss from missing a flight. An arrest report said a 31-year-old woman was charged November 26 with making a false report of planting a bomb. Miami International Airport officials received a call and an e-mail November 25 claiming that a bomb was on an American Airlines plane. Police searched the specified aircraft but did not find a bomb. Investigators tracked the e-mail to the woman's computer. During

questioning, the woman reportedly told police that her boss had been booked on the flight to Honduras, but she had caused him to be late for the flight. She thought the bomb threat would give her boss time to make it. The woman was being held on $7,500 bail.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5in_gUhg5KnmeJPVt_OXLG46M7ALgD9CA3GHG1

21. *December 1, Bloomberg* – (National) **Cargo-screening flaws put fliers at risk, U.S. report finds.** Air passengers may be at risk of terrorist attacks because of air-cargo screening flaws, including a lack of required background checks on freight handlers, according to a U.S. government report. Thirty percent of 6,767 cargo inspections by the Transportation Security Administration found security violations in the three quarters ended in June 2008, according to the Homeland Security Department's inspector general. "Air cargo is vulnerable to the introduction of explosives and other destructive items before it is loaded onto planes, potentially creating risks for the traveling public," he wrote in the report released November 30 in Washington. In all, the Transportation Security Administration recorded 254 violations of access controls, 731 related to security-threat assessments, and 1,655 of security training and testing requirements. Almost a quarter of drivers transporting air cargo did not satisfy testing and training requirements. The inspector general said the report deals with the strengths and weaknesses of the Transportation Security Administration's efforts to secure air cargo during ground transportation and handling before it is loaded onto planes.
Source: http://www.bloomberg.com/apps/news?pid=20601103&sid=arLyVRZNwew8

22. *November 30, Aviation Week* – (National) **FAA bans all polished-frost takeoffs.** Starting January 30, 2010, all aircraft contaminated with "polished" (smooth) frost on wings, as well as on stabilizing and control surfaces will be prohibited from takeoff, according to the FAA final rule published on November 30. Majors and regionals are already prohibited from operating aircraft contaminated with polished frost. FAA's final rule removes language in Parts 91 (subpart F), 125 and 135, which allowed operators to take off with frost that was polished to make it smooth — and requires operators to remove any frost adhering to critical surfaces before takeoff. The final rule also restructures language in parts 91, 125 and 135 to clarify that aircraft must have functioning deicing or anti-icing equipment to fly IFR into known or forecast light or moderate icing — or under VFR conditions into known light or moderate icing conditions. Previous FAA guidance recommended removal of all wing frost prior to takeoff, but allowed frost to be polished smooth if the operator followed the manufacturer's procedures. However, aircraft makers have never published standards of acceptable smoothness, nor is there supportive data to determine how to polish frost to a satisfactory smoothness, according to FAA. The agency makes four recommendations for operators to use to comply with the rule: using wing covers to prevent frost accumulation — which is the least costly method; waiting for frost to melt; keeping aircraft in a heated hangar, or deicing the wing surface. The changes will affect 57 operators and 188 aircraft. Assuming operators would choose using wing covers, FAA estimates the cost of compliance to operators in the 2009-2018 period at

aboout $164,000. Total benefits in the same 10-year period are projected at $980,000. Source: http://www.aviationweek.com/aw/generic/story.jsp?id=news/FROST113009.xml&headline=FAA Bans All Polished-Frost Takeoffs&channel=comm

For more stories, see items **1**, **3**, and **59**

[Return to top]

Postal and Shipping Sector

23. *December 1, Modesto Bee* – (California) **Northeast Modesto post office evacuated.** The Hudson station post office in northeast Modesto was evacuated on December 1 after employees reported an irritating odor in the building, officials said. The Stanislaus County hazardous materials crew went into the building to look for a canister of pepper spray or similar irritant. The odor dissipated and no source was found. The building reopened after emergency crews finished their search. Source: http://www.modbee.com/1618/story/955001.html?storylink=omni_popular

[Return to top]

Agriculture and Food Sector

24. *December 2, Toledo Blade* – (Ohio) **OSHA fines Upper Sandusky feed plant $473,000 for hazards.** Endres Processing Ohio LLC, and its parent company, Endres Processing LLC, of Rosemount, Minnesota received nearly $473,000 in proposed fines from the U.S. Occupational Safety and Health Administration (OSHA) after inspections in the summer found numerous hazards involving dust, the agency said. The company was cited for six willful violations — the agency's most serious rating — and 26 serious violations of the Occupational Safety and Health Act, an agency spokesman said. The willful violations included a lack of explosion protection, failure to equip process equipment with combustible-dust collection systems, hazardous accumulation of dust, and using unsafe electrical equipment in areas with combustible dust accumulation. The situation could have led to an explosion, the spokesman said. Source: http://toledoblade.com/apps/pbcs.dll/article?AID=/20091202/BUSINESS07/912020345/-1/BUSINESS01

25. *December 2, USA Today* – (National) **Why a recall of tainted beef didn't include school lunches.** When health officials identified an August outbreak of salmonella poisonings, they traced the dangerous strain of salmonella to ground beef made at Beef Packers Inc., a major supplier to the National School Lunch Program. At least 39 people reported getting sick in 11 states, and doctors found that the salmonella infections resisted many common antibiotics. On August 6, Beef Packers recalled 825,769 pounds of ground beef made in June at its facility in Fresno, California. The recall covered only ground beef sent to certain retailers. In the days after it was

announced, government and company spokesmen said meat sent to schools was not included. Documents obtained by USA Today through the Freedom of Information Act showed that four orders were produced for the school lunch program during that period. One tested positive for salmonella Newport, the strain that prompted the recall and can cause diarrhea, abdominal cramps, fever and vomiting; that order was rejected by the government. Tests on the other three orders found no salmonella, and the beef was shipped from the plant before the recall was announced. Because samples from the three orders of beef appeared salmonella-free, the meat made for schools was not included in the recall. But lawmakers and food safety experts say the three orders should have been rejected nonetheless. In part, that is because the tests that led the government to release the beef are inconsistent and often wrong, said a professor of food safety and security at Kansas State University. Because salmonella is seldom distributed evenly in any lot of beef, "94% of the time, I won't find it even though it's there," the professor said of testing. "Since one of the four lots tested positive, my recommendation would have been to include all four lots in the recall."
Source: http://www.usatoday.com/news/education/2009-12-01-beef-recall-lunches_N.htm

26. *December 2, Associated Press* – (Idaho) **Idaho cattle herd quarantined after cow tests positive for bacterial disease brucellosis.** The infectious bacterial disease brucellosis has been found in a beef cow in eastern Idaho, and state agriculture officials are scrambling to see if the infection is isolated or if it has spread to other herds. The new assembled herd has been quarantined and is being tested, and epidemiologists are trying to determine the source of the infection, the reporting veterinarian told The Associated Press on Tuesday. None of his cattle had been sold, other than directly to slaughter, the veterinarian assured. The animals came from a variety of sources, including private sales and livestock markets. Officials had not yet determined where the man purchased the infected animal. A spokeswoman for the federal agency that oversees livestock diseases said an investigation has been launched into whether the infection has spread to other herds.
Source: http://www.latimes.com/business/nationworld/wire/sns-ap-us-farm-scene-brucellosis-cattle,0,981021.story

27. *December 1, FOX Business* – (Texas) **FDA warns Tyson about health violations at soup plant.** Regulators from the U.S. Food and Drug Administration (FDA) issued a warning letter to Tyson Foods Inc. (TSN) citing "serious violations" of health regulations at its Fort Worth, Texas seafood soup manufacturing plant. The letter, dated November 13, said the company's seafood soups and sauces were produced in unsanitary conditions. FDA investigators observed "shrimp and crab meat thawingâ ¦at temperatures between 40-55 degrees for approximately 18 hours, in preparation for manufacturing your firm's Seafood Gumbo," regulators told Tyson. The FDA said the meat should be stored at temperatures below 40 degrees the company to prevent the growth of pathogens. A spokesman from Tyson told Dow Jones that "Contrary to the impression left by the FDA letter, our Fort Worth plant is clean and sanitary and the products produced there are safe to eat."

Source: http://www.foxbusiness.com/story/markets/industries/industrials/fda-warns-tyson-health-violations-soup-plant/

28. *December 1, Associated Press* – (North Carolina) **N.C. safety regulators cite ConAgra in plant blast.** North Carolina workplace inspectors have cited factory owner ConAgra and a contractor for dozens of serious safety violations in the June explosion at Slim Jim plant that killed four people. The state Labor Department said Tuesday it cited ConAgra Foods for 26 serious violations and fined the company nearly $135,000. Regulators also faulted a Hickory company hired to install a water heater at the plant. Energy Systems Analysts Inc. was cited for 28 serious violations and fined $58,000. Two federal agencies have blamed natural gas for the blast. The Chemical Safety Board said contractors installing a 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.
Source: http://www.news-record.com/content/2009/12/01/article/nc_safety_regulators_cite_conagra_in_plant_blast

29. *December 1, USA Today* – (National) **Invasive carp threatens Great Lakes.** Fish and wildlife officials will poison a 6-mile stretch of water near Chicago on December 2 in a last-ditch effort to keep one of the most dangerous invasive species of fish, the Asian carp, out of the Great Lakes. The Asian carp now dominates the Mississippi and Illinois rivers and their tributaries. The fish has entered the Chicago Sanitary and Ship Canal and is knocking on the door of Lake Michigan. Once inside a Great Lake, the carp would have free rein in the world's largest freshwater ecosystem, imperiling the native fish of the lakes and a $7 billion fishing and recreation industry. "We've got a chance to beat this thing, but we've got to do everything right," says the acting president of the Alliance for the Great Lakes, a conservation group. The poisoning will kill an estimated 100 tons of fish, which will be removed by crane and hauled to a landfill. The five-day fish kill will provide time for the Army Corps of Engineers to perform routine maintenance on an electrical barrier that has been placed in the canal to block Asian carp from entering Lake Michigan. No Asian carp have been found on the Great Lakes' side of the electrical barrier. However, recent DNA samples taken from water indicate the carp may have gotten past the barrier. The Great Lakes' last line of defense is the world's largest electrical fish barrier, constructed in the Chicago Sanitary and Ship Canal.
Source: http://www.usatoday.com/news/nation/2009-11-30-asian-carp_N.htm

[Return to top]

Water Sector

30. *December 2, Newark Advocate* – (Ohio) **Operator has had 56 violations of regulations.** Since 2001, David R. Hill Inc. has had 56 violations of agency regulations on the 247 oil and gas wells it owns in Ohio, according to Ohio Department of Natural Resources (ODNR) records. The greatest number — about 15 — were for oil spills on

the ground in the immediate vicinity of the well. Others included failing to plug a well that was no longer in operation and failure to identify the well with a legible number. That hinders the agency's response to an emergency at the site, said the deputy chief of the agency's Division of Mineral Resources Management. All of the violations were what he called "repair and maintenance issues." To prevent infiltration of oil or gas into the aquifer ODNR requires insertion of steel piping — cemented to the drill hole — that extends from ground level to the oil and gas deposits. To guard against surface water contamination, the agency requires cuttings and other residue from drilling be placed in a plastic-lined pit located next to the drill hole. A dike surrounding oil storage tanks that is capable of holding 150 percent of the volume of the tanks must be constructed. Although he could not determine if any of the 56 violations presented danger to the aquifer, he said there is no record of any citizen complaints involving contamination of ground or surface water from David R. Hill operations. The president of David R. Hill Inc. said he has had no violations at the roughly 25 wells he operates in urban areas, although that could not be confirmed by ODNR.
Source:
http://www.newarkadvocate.com/article/20091202/COMMUNITIES02/912030314

31. *December 2, Amarillo Globe News* – (Texas) **500,000 gallons of effluent spill.** City officials continued mopping up a sewage spill in southeast Amarillo on Tuesday as they began to analyze what caused the pipeline to rupture for the second time this year. A break that occurred Monday in the 16-inch-diameter force main at Southeast 58th Avenue and Osage Street led to the release of an estimated 500,000 gallons of sewage into barrow ditches running parallel to Southwest 58th. The break occurred only 20 feet from the spot where the pipe broke in March, sending about 600,000 gallons of sewage into the area, the city Water and Sewer superintendent said. No residences were affected by either spill, according to information from the city. The age of the pipeline is not a likely cause of the breaks, he said. The city is investigating whether the pipe, which lies about 5 feet below the surface, had been damaged by contractors working in the area through the years. The pipeline section also "bends," or changes alignment, in the area, so internal pressure on the pipe — it is called "water hammer" — at a stress point is another possibility, he said. Wastewater collection department crews completed a repair on the force main by midnight Monday, the city statement said. The city is awaiting results of lab tests on samples of water from Southeast Lake in Southeast Park to determine if any of the sewage reached the lake. In the meantime, a road inside the park that leads to the lake has been closed to the public to restrict access. He said the initial staff recommendation would be to lay a new line parallel to the existing one. Engineers are studying the feasibility of the proposal.
Source: http://www.amarillo.com/stories/120209/new_news3.shtml

32. *December 1, U.S. Environmental Protection Agency* – (Colorado) **EPA cites Bucklen Equipment for damages to the Cache la Poudre River in Greeley.** The U.S. Environmental Protection Agency (EPA) has reached an agreement with Bucklen Equipment Company, Inc. to resolve alleged violations of the Clean Water Act in Weld County, Colorado. The alleged violations include unauthorized discharges of pollutants to the Cache la Poudre River and its adjacent wetlands within the City of Greeley.

Under the consent agreement, the company will pay a penalty of $16,000 and will remove any remaining gravel piles from wetlands along the river. “Bucklen Equipment’s actions introduced a source of sediment pollution and altered the condition of the Poudre River and its nearby wetlands,” said the director of EPA’s Water Enforcement program in Denver. In August 2008, the U.S. Army Corps of Engineers (Corps) received information that Bucklen Equipment was conducting extensive excavation activities in the Cache la Poudre River, including the removal of islands and grading of the river’s floodplain. Subsequent investigation by the Corps and EPA found that the company had deposited dredged and fill material in an area encompassing 1,400 feet of the river’s length without authorization. The Corps and EPA identified areas that had been dredged and filled in both the river and adjacent wetlands. Under the consent agreement, Bucklen Equipment will remove any remaining piles of fill in wetlands along the banks of the Cache la Poudre River. EPA will inspect the area next summer to determine if the area has properly recovered. If it appears that additional work such as re-contouring or planting vegetation is required, Bucklen Equipment may be directed to submit and implement a restoration plan.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/F86FAF3C1DD9E57D8525767F006E5690

33. *December 1, Water Technology Online* – (Louisiana) **Brown water should be a thing of the past.** A $6 million project now is under way to replace virtually all of this northeast Louisiana community’s collapsing cast-iron water pipes, a project which should result in clearer-running tap water, The News-Star reported December 1. Local, state, and federal officials on November 30 broke ground on the second part of a two-phase project, much of which is being paid for by a U.S. Department of Agriculture grant and loan. The town recently upgraded its water treatment plant. The mayor is quoted in the story saying, “We’ve been plagued by brown water forever. It’s been a problem that needed to be addressed for decades, so this is a great day for Rayville.”
Source: http://watertechonline.com/news.asp?N_ID=73024

34. *December 1, Staten Island Advance* – (New York) **Illegally discharged substance likely cause of Port Richmond plant evacuation.** Approximately 140 employees were evacuated from a wastewater treatment plant in Port Richmond, New York, the morning of December 1 after an “illegally discharged substance” — likely a petroleum product dumped into the sewer system — entered the facility, a spokeswoman for the city Department of Environmental Protection (DEP) said. Two electricians were treated by EMS and taken to Richmond University Medical Center, West Brighton, according to a DEP spokeswoman. The source of the discharge remains under investigation. Workers said the fumes smelled like gasoline. One worker said he saw one of the electricians removed by stretcher after collapsing. “We were working, and he was just overcome with fumes,” he said.
Source:
http://www.silive.com/northshore/index.ssf/2009/12/illegally_discharged_substance.html

For another story, see item **29**

[Return to top]

Public Health and Healthcare Sector

35. *December 2, Washington Post* – (National) **Fed to review policy after vaccine shortage.** A top administration official, citing problems with the swine flu vaccination campaign and other shortcomings in preparedness, announced plans Tuesday for a major review of the federal government's policies for developing public health defenses. The Health and Human Services Secretary said she had ordered the review in part because the swine flu vaccine shortage had highlighted the nation's dependence on antiquated technology. "Under the review I've announced today, we'll look for the fastest ways to move to new technologies that will let us quickly produce countermeasures that are more dependable and more robust," she said in prepared remarks to the American Medical Association's Third National Congress on Health System Readiness in Washington. The nation's ability to respond to such threats depends not only on having enough hospital beds, emergency rooms, doctors and equipment such as masks and ventilators, but also on state-of-the-art diagnostic tests, medications and vaccines, she said.
Source: http://detnews.com/article/20091202/LIFESTYLE03/912020358/Fed-to-review-policy-after-vaccine-shortage

36. *December 1, KWTX 10 Waco* – (Texas) **Patients evacuated after smoky fire breaks out in old Hillcrest hospital.** Waco, Texas, firefighters responded Tuesday to a report of a fire in the first-floor kitchen area of the old Hillcrest Baptist Medical Center building at 3000 Herring Ave. Most of Hillcrest's operations were moved earlier this year to the new campus, but 22 assisted-living and rehab patients were in the building. They were evacuated to the lobby area, primarily because of the smoke.
Source: http://www.kwtx.com/home/headlines/78252232.html

37. *December 1, Business Journal of Milwaukee* – (Wisconsin) **Wisconsin to create electronic medical records exchange.** The state of Wisconsin will develop an operational plan for an electronic medical records exchange by June 1, 2010, the governor announced Tuesday. He said the creation of the Wisconsin Relay of Electronic Data (WIRED) for Health Board will make the exchange possible and make it easier to transfer medical records from one hospital to another, he said during a press conference at Aurora Sinai in Milwaukee. He said the move also sets a framework for legislative action to establish a nonprofit entity to implement the plans for using and exchanging electronic records when the Legislature reconvenes in 2010. Wisconsin is receiving $9.44 million in American Recovery and Reinvestment Act funds to support efforts to create a state exchange. The Recovery Act provides an additional $34 billion in incentives for hospitals to begin using electronic records.
Source: http://milwaukee.bizjournals.com/milwaukee/stories/2009/11/30/daily28.html

For another story, see item **51**

[Return to top]

Government Facilities Sector

38. *December 2, Fox News* – (International) **Russian satellite debris zooms by space station.** A tiny piece of a defunct Russian satellite passed by the International Space Station Tuesday, but was far enough away that outpost's two-man crew did not have to strap into their lifeboat to wait out the close shave, NASA officials said. The debris — a small piece of a Cosmos satellite less than four inches wide — zoomed by the station at 1:19 p.m. EST and came within a mile of the outpost at its closest point. NASA detected the object too late to move the space station clear of the incoming space trash by firing its thrusters. Instead, NASA told the station's American commander and Russian flight engineer that they might have to wake up during their sleep period and take refuge in their Soyuz spacecraft. The Russian-built Soyuz vehicles ferry crews to and from the station, and also serve as lifeboats in case astronauts must leave the orbiting laboratory in an emergency. But additional analysis of the object's trajectory found that, despite its close pass, the satellite remnant posed no danger of hitting the space station. NASA typically moves the space station if there is a 1-in-10,000 chance of an object striking the $100 billion orbiting laboratory.
Source: http://www.foxnews.com/story/0,2933,578715,00.html?test=latestnews

39. *December 2, Texarkana Gazette* – (Arkansas) **Military responds to bomb threat.** What an anonymous caller promised was a bomb in the parking lot of the Miller County jail Tuesday was revealed as a fake by military experts operating a robot. "It had all the appearances of an explosive device, but this was a hoax device," said the Miller County sheriff. In less than an hour, a five-man, one-robot Air Force Explosive Ordnance Disposal team examined the contents of the package. They drove away from the Miller County jail in Texarkana, Arkansas, shortly after 11:30 a.m.
Source: http://www.texarkanagazette.com/news/localnews/2009/12/02/miller-county-military-responds-to-bomb--31.php

40. *December 1, Reuters* – (District of Columbia) **Secret Service probe package near White House.** The U.S. Secret Service said on Tuesday they were investigating a suspicious package near the White House complex and a few nearby streets were closed. The incident was at 15th Street and Pennsylvania Ave., NW which is near the U.S. Treasury Department and a block from the White House, the Secret Service and the D.C. Fire Department said.
Source:
http://www.publicbroadcasting.net/wbfo/news.newsmain/article/0/0/1583737/US/Secret.Service.probe.package.near.White.House

41. *December 1, Associated Press* – (South Carolina) **Lt. Gov. candidate Connor Web site hacked.** A Columbia attorney who is running for lieutenant governor claims his campaign Web site was defaced by an unidentified Middle Eastern hacker promoting radical Islam. However, a computer expert says it is impossible to determine where the hacker was based. The changed site included a black screen with some red script in

English saying, “This is hacked and owned,” identifying a Dr. HiaD as the hacker. The hacked page also had green comments with some profanity and a small bit of Arabic script. The Republican’s site was back up Tuesday, less than a day after the intrusion. In a statement, he declared that such a threat would not keep him from doing his job. A computer expert contacted by the Associated Press who studied the site says the alterations are similar to those made about 4,500 times elsewhere on the Web. In a statement issued Tuesday, the attorney said the hacking incident was apparently connected to his military service in Afghanistan. The 41-year-old lawyer is an Army Reserve lieutenant colonel who wrote a book about his experiences commanding an Army Ranger unit.
Source: http://www.telegram.com/article/20091201/APN/312019328

[Return to top]

Emergency Services Sector

42. *December 2, KPRC 2 Houston* – (Texas) **Fingerprinting problems found in Houston.** The Houston Police Department (HPD) found serious problems in its Latent Print Unit when it tried to get it accredited, resulting in thousands of violent crime cases going under review, KPRC Local 2 reported Tuesday. The Houston Police Chief said that an audit of the fingerprinting lab showed a lack of staffing, supervision and training. Consultants were hired to assess the operational readiness, staffing and resource capabilities to see if the department complied with American Society of Crime Laboratory Directors - Laboratory Accreditation Board standards. The department said it identified several problems including insufficient staffing, lack of proper supervisory review, inadequate quality control/quality assurance protocols, technical competence inconsistent with industry standards, insufficient training and inadequate standard operating procedures. “The results of the technical audit were mixed. On the plus side, there were no erroneous identifications,” he said. While no one has been falsely identified by fingerprints, he said the audit found what he called an unacceptable number of errors. “That’s a situation where you actually have a print on a piece of evidence and they just missed it,” said the HPD’s executive chief. The department said it has taken action to solve the problems. One employee has been fired and three others, including a supervisor, have been placed on administrative leave. HPD said it will review all violent criminal cases for the past six years, including homicides and sexual assaults. The audit also found a backlog of 6,000 cases and blamed it on insufficient staffing and training along with inadequate standard operating procedures. The review process could take two years.
Source: http://www.officer.com/online/article.jsp?siteSection=1&id=49583

43. *December 2, Jersey Journal* – (New Jersey) **Emergency drills from 9 to 11 today in Hudson.** The New Jersey State Police and the New Jersey Office of Emergency Management conducted emergency drills Wednesday in seven counties, including Hudson County. The drills were designed to test first responder deployment. The locations of the drills were not announced, but the public will not be involved or alarmed, a State Police spokesman said.

Source: http://www.nj.com/news/jjournal/index.ssf?/base/news-4/125973874132280.xml&coll=3

44. *December 1, KSL 5 Salt Lake City* – (Utah) **Davis County Jail to use eye scanners on inmates.** There is a plan in Davis County to keep the wrong people from leaving jail after a couple of high-profile mistakes. The Davis County Sheriff's Office is the first in the country to receive a $10,000 grant to start using an eye scan system to keep track of jail inmates. The eye scans are stored in a national database and can quickly be pulled up to make sure a person is who they say they are. A year ago Davis County accidentally released a wrong inmate. They are hoping this new system will make sure that never happens again. Some say the eye scan system should also be used to help find missing kids or elderly adults who might wander off and forget who they are.
Source: http://www.ksl.com/?nid=148&sid=8869316

45. *December 1, Elk Grove Citizen* – (California) **Homeland Security funding to support city emergency communications center.** When Congress approved this year's Homeland Security spending, a piece of the pie was set aside for Elk Grove. The 2009-10 federal Homeland Security Appropriations Bill, signed in late October, included a $750,000 Federal Emergency Management Agency (FEMA) earmark for an emergency operations center in Elk Grove. The center would be a communications hub used by various agencies to coordinate the response to a large-scale disaster. A representative who sits on the House Committee on Homeland Security and represents Elk Grove in Congress said the funding helps address a federal concern and a local interest. "There's been a problem with respect to coordinating operations (when responding to a disaster)," he said in a November 13 phone interview. "Part of that difficulty in coordinating operations in a regional area was a lack of communications capability." The operations center will be housed in Elk Grove's City Council Chambers, and will only be used when the emergency procedures are authorized by the city manager, according to the Elk Grove city spokesperson. The $750,000 will pay for renovations to the chambers like an emergency generator, electrical and data ports, fiber optic cables and conduit, she said. The funding will also provide for video cameras that would provide views of traffic at major intersections and roadways leading into and out of the city to relieve traffic congestion as well as "locations determined to be 'sensitive' for the purposes of Homeland Security," according to a January Elk Grove staff report spelling out the city's request for the funding.
Source:
http://www.egcitizen.com/articles/2009/12/01/news/doc4b15b69da8110810506883.txt

46. *November 30, Tech Crunch* – (Washington) **Another Google Wave use: manhunt.** Tech Crunch reported that the Seattle Times set up an area on the newly released Google Wave aimed at catching the man who was suspected of killing four Seattle police officers. Within an hour over 100 people had joined and were posting in the effort. Included were Wave elements with links to police scanner audio, live video footage of the search, a suspect description, and information about local schools on lockdown.
Source: http://www.techcrunch.com/2009/11/30/google-wave-

manhunt/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Techcrunch+(TechCrunch)

[Return to top]

Information Technology Sector

47. *December 2, Homeland Security News Wire* – (International) **New report: The line between cybercrime and cyberwar is blurred.** Organized Internet-based crime has reached such intensity and scale that the distinction between cybercrime and cyberwar is being blurred, security giant McAfee said in its annual Virtual Criminology Report. "Is the age of cyberwar at hand?" McAfee asked in the report, citing evidence that countries hostile to industrial democracies are involved in some of the more serious and sustained cybercrime. In response, McAfee said, "nation-states are arming themselves for the cyberspace battlefield." The number of reports of cyberattacks and network infiltrations that appear to be linked to nation-states and political goals continues to increase, McAfee said. "There is active debate as to when a cyberattack reaches the threshold of damage and disruption to warrant being categorized as cyberwarfare," said the report. "With critical infrastructure as likely targets of cyberattacks, and private company ownership of many of the information systems in these sectors, private companies will likely be caught in the crossfire," the report warned. The CEO of McAfee said, "Experts disagree about the use of the term 'cyberwar,' and our goal at McAfee is not to create hype or stoke unwarranted fear. But our research has shown that while there may be debate over the definition of cyberwar, there is little disagreement that there are increasing numbers of cyberattacks that more closely resemble political conflict than crime. McAfee believes the private sector at large needs to prepare for cyberattacks, and "those businesses that can weather the storm better than their competitors could be in a position to gain considerable market share." McAfee also called for greater transparency in current discussions on combating cybercrime. The report said, "Too much of the debate on policies related to cyberwar is happening behind closed doors."
Source: http://homelandsecuritynewswire.com/new-report-line-between-cybercrime-and-cyberwar-blurred

48. *December 1, DarkReading* – (International) **US-CERT warns of VPN attack that bypasses browser security.** The US-CERT has issued an advisory on a vulnerability in SSL VPN products that breaks basic browser security features, letting an attacker bypass authentication steps and wage other Web-based attacks. There is no known fix for the problem, according to the advisory, but US-CERT offers several workarounds to mitigate an attack that exploits the vulnerability. The advisory affects some SSL VPNs that allow browser-based — rather than VPN client-based — access to intranets and external Web resources. This type of Web-based VPN is typically used for internal Webmail server access, file shares, and remote desktop tools. Users connect to the VPN via their Web browser, which authenticates them to their VPN. A user first has to be duped into viewing an attacker's infected Web page, where the attacker then can grab the user's VPN session tokens and read or alter the victim's cookies or HTML content.

"This effectively eliminates the same origin policy restrictions in all browsers. For example, the attacker may be able to capture keystrokes while a user is interacting with a web page. Because all content runs at the privilege level of the web VPN domain, mechanisms to provide domain-based content restrictions, such as Internet Explorer security zones and the Firefox add-on NoScript, may be bypassed," the US-CERT advisory says. Security experts say the actual threat to enterprises all depends on how they've configured their VPNs. "In the end the risk will be different for every organization, depending on the setup they're using. I actually think this is a time when the risk is broad enough that calling this serious or not is entirely opinion-based, as it needs to be judged on a case-by-case basis," says the lead security research engineer at nCircle. "This isn't really a vulnerability — it's a weakness."
Source:
http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=222000105

49. *December 1, Nextgov* – (International) **Survey shows cyberattacks are getting more disruptive.** Cyberattacks that seek to penetrate computer networks or disrupt online services are increasing significantly, according to a survey of public and private sector information security and technology professionals released on December 1. Infections from software designed to infiltrate or damage a computer system were "easily the most prevalent" type of cyberattack in 2009, the Computer Security Institute survey found. More than 64 percent of 443 respondents said they were victims of malware attacks, compared to 50 percent in 2008. Often these were multistage attacks, in which the malware downloaded separate tools to enhance the severity of the infection once inside the network, according to the report. Eight percent of survey participants, or 34 people, worked for the federal government. The San Francisco-based association noted that reports of malware infection are likely to continue climbing as attackers "spend more energy customizing malware to make it more effective in targeted attacks." Twenty-five percent of survey respondents reported at least some of their security incidents involved targeted attacks, and 4 percent said they experienced more than 10 such infiltrations. Conversely, 34 percent of respondents were fraudulently represented as senders of phishing messages that tricked recipients into clicking a link or downloading an attachment that installed malicious software.
Source: http://www.nextgov.com/nextgov/ng_20091201_5149.php

50. *December 1, The Register* – (International) **Anti-spammers urged to gang up.** The combined efforts of anti-spam products outperform any individual products alone, according to an experiment by Virus Bulletin, the independent security certification organization. In a comparative test, almost 200,000 sample emails were sent to 14 different anti-spam products that were required to filter out spam messages from legitimate smails (ham). The test found that no legitimate mail was blocked by more than four products. The tests gave VB's anti-spam team the idea of a hypothetical spam filter that marked email as spam if at least five of the 14 products evaluated marked it as dodgy. Such a hypothetical filter would achieve a capture rate of 99.89 percent and, better still, no false positives. "For end-users this means that if spam filtering is business-critical, the use of more than one spam filter may be a good option," said

VB's anti-spam test director. "The anti-spam industry, meanwhile, should consider the benefits of collaboration and information sharing — and might be better able to protect our inboxes as a result." "Every spam filter uses multiple techniques but their effectiveness could be further improved if vendors share information on the latest spam attacks between each other more efficiently," the test director explained. The bimonthly VBSpam tests use Virus Bulletin's live email feed as well as spam messages provided by Project Honey Pot. Each tested product is exposed to the same email stream. Source: http://www.theregister.co.uk/2009/12/01/anti_spam_mashup_tests/

51. *December 1, CNET News* – (International) **Fake CDC vaccine e-mail leads to malware.** An e-mail that looks like it comes from the U.S. Centers for Disease Control and Prevention (CDC) about creating a profile for an H1N1 vaccination program is a malware scam, according to security provider AppRiver. The fake alert informs recipients that as part of a "State Vaccination H1N1 Program" they need to create a profile on the CDC Web site. The link in the e-mail goes to a fake CDC page where the visitor is assigned a temporary ID and a link to a vaccination profile that is actually an an executable file containing a copy of the Kryptik Trojan targeting Windows, according to an AppRiver blog post on Tuesday. Once installed, "this Trojan will create a security-free gateway on your system and will proceed to download and install additional malware without your authorization," the post warns. "It also enables a remote hacker to take complete control of your computer. This malware can log your typed keystrokes and send confidential personal and financial data (including banking information, credit card numbers, and website passwords) to a remote hacker." AppRiver said it was seeing the fake CDC e-mails at a rate of nearly 18,000 messages per minute, reaching more than 1 million in the first hour alone. The malware campaign apparently got more dangerous as the day wore on. In later iterations of the fake CDC e-mail, the landing page that the link led to contained a hidden iFrame that pointed to a site hosted in Ukraine, according to Symantec. In the background, the iFrame checks to see if the system is running an unpatched version of Adobe Reader, Acrobat or Flash Player and if so it uses an exploit to download a file to the system, the company said. Source: http://news.cnet.com/8301-27080_3-10407026-245.html

52. *November 30, BBC* – (International) **Runescape creator pursues 'phishing thieves'.** A British man has been arrested and cautioned for stealing accounts for online game Runescape. Jagex, creator of Runescape, said it was likely to be the first of several arrests as it tackled in-game fraud. Online game Runescape has more than 100 million active players and play revolves around collecting and spending virtual cash and loot. The company said it was working with U.K. police and the FBI to track down and catch those targeting Runescape. A statement from the Police National e-crime unit said: "A 23-year-old man was arrested in Avon and Somerset on the morning of Tuesday 24 November by officers from the Police Central e-crime Unit, on suspicion of a number of computer misuse offences." The offenses are believed to be for using phishing e-mails to trick people into handing over login details for Runescape accounts. Once hi-tech thieves have these credentials, they plunder the accounts, strip characters of their items and sell off the rare virtual goods for Runescape gold. This virtual money can be traded to others in-game or sold for real world cash. Current underground

exchange rates suggest that 2m Runescape gold costs about Â£6 ($10). “Any online games company will tell you that as soon as the game has value, there’s a very small foreign element that tries to exploit that value,” the chief executive of Jagex told BBC News. “Players invest years of time and effort into developing their Runescape character so the theft of a Runescape account shouldn’t be treated differently to the theft of any other valuable possessions such as a games console, television or car,” the chief executive said.
Source: http://news.bbc.co.uk/2/hi/technology/8386003.stm

53. *November 3, The Register* – (International) **Russian ransomware blocks net access.** Miscreants have developed a ransomware package that blocks internet access in a bid to force infected users into paying up by sending a text message to a premium rate SMS number, lining the pocket of cybercrooks in the process. The malware comes bundled in a package called uFast Download Manager and targets potential marks in Russia. Users of infected machines are told (via a Russian language message) that they need to send a text message in order to obtain an activation code for the product, which (ironically) poses as a software package designed to increase download speeds. Victims are told that internet access has been blocked in the meantime because of supposed violations of a licensing agreement. The ploy is a variant on previous ransomware packages that encrypt and block access to document files. One strain of ransomware detected in January 2008 locks up Windows machines, seeking payment via SMS. That threat wasn’t specific to Russia and didn’t affect a net connection as such but is otherwise very similar to the latest attack. CA, which detects the threat as RansomSMS-AH, explains how the malware works in greater depth in a blog posting featuring screenshots culled from infected machines here. The anti-virus vendor has developed an activation code generator that allows victims to get online again - providing they can download the utility through an uninfected machine first, of course.
Source: http://www.theregister.co.uk/2009/12/01/ransomware_turns_off_net_access/

For more stories, see items **41** and **54**

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. *December 2, CNET News* – (International) **McAfee uncovers riskiest domains.** The .cm domain, which belongs to Cameroon, was pegged by McAfee as the world’s riskiest domain. McAfee’s third annual “Mapping the Mal Web” report, released Wednesday, looks at riskiest and safest domains across the globe. The small nation on

the west coast of Africa reached the top spot this year with 36.7 percent of its sites posing a security risk. Because .cm is often a typo for .com, McAfee said, cybercrooks like to use that domain to set up typo-squatted sites to hit you with malware. The generic and widely used .com domain itself is not much safer, according to McAfee, jumping from ninth last year to second this year in riskiness, with 32.2 percent of its sites potentially hazardous to a user's PC's health. Romania (.ro) is tagged as the riskiest domain for malicious downloads, with 21 percent of its sites delivering payloads of viruses, spyware, and adware. The information (.info) domain is seen by McAfee as the most "spammy," with 17.2 percent of its sites generating junk mail. On the positive side, the government (.gov) is the safest generic domain with essentially 0 percent risk, while Japan (.jp) proved the safest country domain with a rating of only 0.1 percent. Last year, Hong Kong was the riskiest domain and this year it is dramatically safer," the chief technology officer for McAfee Labs said in a statement. "Cybercriminals target regions where registering sites is cheap and convenient, and pose the least risk of being caught." Overall, looking at 27 million Web sites and 104 top-level domains, McAfee found that 1.5 million sites, or 5.8 percent, were risky. That is up from 4.1 percent from the past two years, although the comparison is not direct since McAfee said it changed its rating methodology since then. McAfee noted that cybercriminals who create domains to scam people prefer registrars with cheap prices, volume discounts, and hefty refund policies. Crooks also like registrars with a "no questions asked" policy and that act slowly or not at all when informed of malicious domains.
Source: http://news.cnet.com/8301-1009_3-10407530-83.html

55. *December 1, CNET News* – (International) **India blocks service to millions of handsets.** India has blocked service to all mobile phones without a valid identity code, as part of antiterrorist measures being implemented by the Indian government. On Monday, any handset without a valid International Mobile Equipment Identity (IMEI) code had its connection cut off, according to the Indian Cellular Association (ICA), which represents mobile operators in the country. The mobile industry is complying with a government directive that arose after discussions between Indian security agencies and the Indian Department of Telecommunications, the ICA added. The IMEI, a 15-digit number printed inside a phone, can be used to identify a particular device on an operator's network, meaning it can be tracked by security services. In addition, network providers can use the absence of an IMEI to cut off a phone.
Source: http://news.cnet.com/8301-1035_3-10406985-94.html

56. *December 1, Network World* – (National) **Data center start-up Arista expands Gigabit Ethernet switch line.** Arista Networks has unveiled a Gigabit Ethernet data center switch designed to better accommodate increasing traffic loads between the server access and core layers of the network. The high throughput and bursty traffic patterns of storage, video, market data feeds and Web 2.0 applications present challenges to the network in terms of speed mismatches, reliable congestion management and consistent performance. To address that, the Arista 7048 multilayer switch is a fixed-configuration 1RU device that sports 48 wire-speed 100/1000BASE-T Ethernet RJ-45 ports with four SFP+ 1/10Gbps Ethernet uplinks. It supports up to

40Gbps of interconnect capacity to switches in the core, or "spine" of the network. The switch also integrates Citrix Systems' NetScaler VPX load balancing and application security software to divvy up traffic loads across servers within a rack. VPX operates as a virtual load balancing appliance with the switch, Arista says. The 7048 also features large buffers on each port that, combined with non-blocking operation and load balancing, help the switch manage congestion during peak traffic loads. Total shared packet memory on the switch is 768MB. Like the existing Arista 7100 line of 1/10Gbps Ethernet data center switches, the 7048 runs the company's EOS operating system, which supports access to Linux tools, extensible network services and integration with third-party applications such as Citrix NetScaler VPX. It also features high-availability features such as stateful fault repair and in-service software upgrades, Arista says.
Source: http://www.computerworld.com/s/article/9141640/Data_center_start_up_Arista_expands_Gigabit_Ethernet_switch_line

[Return to top]

Commercial Facilities Sector

57. *December 2, Minnesota Public Radio* – (Minnesota) **Copper thieves leave $10,000 in damage at Midway Stadium.** Thieves who forced open eight breaker boxes to steal copper along the outfield wall at the St. Paul Saints baseball stadium left about $10,000 in damage, officials said Wednesday. Police were called Monday about the theft at Midway Stadium, which is believed to have taken place Sunday night or early Monday, a St. Paul Police spokeswoman said. Wires inside the breaker boxes were pulled or cut, and copper was missing. The boxes themselves were also damaged. She said the thieves did not leave much that would help police solve the crime. Thieves made away with copper from the same place almost two years ago, so stadium officials are looking for ways to improve security, said a spokesman for the St. Paul Parks and Recreation Department. The city owns the stadium, which is rented by the St. Paul Saints. There are currently no security cameras that would have recorded the incident, and the parks department is working with police to find ways to improve surveillance, he said. Right now, one method is having police officers with dogs stop by the stadium complex at night to walk them, he said. "Our resources are already stretched pretty thin," he said, adding that it would be difficult to having security personnel stationed at the stadium each night. City officials are now trying to figure out how much insurance will pay for the damage and whether to replace the wiring now or wait until the weather improves, he said.
Source: http://minnesota.publicradio.org/display/web/2009/12/02/copper-thieves-hit-midway-stadium/

58. *December 1, Arizona Republic* – (Arizona) **'Suspicious' chemicals found inside storage unit.** The area around a Phoenix storage unit was evacuated Tuesday after a new owner found "suspicious" chemicals inside. Although authorities are stopping short of calling the unknown substance methamphetamine, the chemicals "appear to be the chemicals involved in illicit trades," said the captain of the Phoenix Fire

Department. The building was evacuated and officials established quarantine around the area, the captain said. No nearby homes were evacuated. The investigation has been turned over to Phoenix police.
Source: http://www.azcentral.com/news/articles/2009/12/01/20091201abrk-materialspill.html

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

59. *December 2, Dallas Morning News* – (Texas) **Corps of Engineers allows bridge, but levees will need repairs.** The U.S. Army Corps of Engineers has determined that the Margaret Hunt Hill Bridge over the Trinity River levees can be built without damaging Dallas' flood control system. Plastic sheets cover what looked like a giant bite in the levee near Stemmons Freeway. The mayor played down the cave-in as he emphasized the new bridge. City leaders on Tuesday hailed the decision on the bridge, a signature element of the troubled Trinity River project. Its soaring 40-story white arch is expected to transform the Dallas skyline. Earlier this year, the corps halted construction of the bridge's approaches between Woodall Rodgers Freeway and Singleton Boulevard because of concerns that support piers built into the levees could compromise their integrity and damage the floodway system. Still, the Texas Department of Transportation — which is overseeing the bridge's construction — went forward with building the bridge's main expanse. The city still faces a mandate to make significant repairs and upgrades to the levees that protect Dallas from catastrophic flooding. Even as many at City Hall celebrated the announcement that the $117 million bridge will be finished, there was a stark reminder of the levees' potential fragility. A section of a levee near Regal Row and Stemmons Freeway caved in this week after a 48-inch water main that runs beneath it broke open.
Source: http://www.dallasnews.com/sharedcontent/dws/news/localnews/stories/DN-trinity_02met.ART.State.Edition2.4bb5e72.html

60. *December 1, St. Louis Post-Dispatch* – (Missouri) **Corps comes up with emergency plans for levee.** The Army Corps of Engineers has developed emergency plans that would be used to combat seepage under a Mississippi River levee if high waters return before a permanent fix for the problem can be implemented next year. Working with local officials, the Corps would build dikes and increase water levels in the wetland behind the earthen levee, creating pressure that would stop seepage and possible undermining of the levee, the commander of the corps' St. Louis District told local officials at a meeting. He said there is no imminent threat of levee failure but work on a permanent remedy is urgent and should start with the beginning of the construction

season next spring. He said the work would take two or three months and could cost as much as $30 million. He said engineers believe the problem was caused by construction of the Melvin Price Locks and Dam in the early 1990s, so the cost of repairs would be entirely borne by the federal government. The problem area is on the Illinois side of the river just upstream from the locks and dam. A survey party in August discovered sand boils 200 to 300 feet inland from the levee, where they were not expected to occur. Sand boils form when hydraulic pressure forces water and, sometimes, sand to flow under a levee and boil up up on the inland side. He said only clear water was flowing through the sand boils in August, which was not a great concern. In October, however, sand was moving through the boils, which is a serious concern. Any movement of solid material undermines the levee and the amount of undermining that has occurred is unknown, he said. “We don’t know how long this has been going on,” he said. “That’s why we’re treating this with such a sense of urgency.” Two permanent solutions are under consideration: a “cutoff wall,” a 6,500-foot-long poured concrete wall running down the center of the levee and resting on bedrock; or a 4-to-6-foot deep “sand berm” that would be placed over the area behind the levee where sand boils have erupted. The latter option would eliminate about 60 acres of wetland that supports abundant wildlife.
Source:
http://www.stltoday.com/stltoday/news/stories.nsf/illinoisnews/story/D5E4887A67CA41228625767F00674608?OpenDocument

[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