Department of Homeland Security Daily Open Source Infrastructure Report for 04 January 2006

Current Nationwide Threat Level is ELEVATED — Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports the West Virginia coal mine where 13 miners were trapped after an explosion Monday, January 2, was cited 208 times for alleged safety violations in 2005, up from 68 citations the year before. (See item 3)
- Wireless reports Fiberlink Communications has released a free video, "Anatomy of a Hack," that details what it calls ongoing security risks and vulnerabilities that threaten mobile workers. (See item 8)
- The Washington Post reports Flyi Inc., parent of Dulles−based low−fare airline Independence Air, said it will discontinue flights after Thursday evening, January 5, because it cannot find a buyer for its financially troubled operation. (See item 13)

Energy Sector

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

1. *January 03, T&D Magazine* — **California utility crews work to restore power after three back−to−back storms.** As the third in a series of strong Pacific storms batter northern and central California over the New Year's holiday, Pacific Gas and Electric Co. (PG&E) crews worked to restore power, and repair damage to electric equipment throughout the affected area.

As of 9 p.m. PST, Monday, January 2, approximately 87,000 PG&E customers were without power throughout northern and central California −− the majority in the Humboldt, Fresno, Bakersfield, and San Luis Obispo regions. Since the storms began, more than 2,500 locations have experienced equipment damage requiring repairs. In total, 269 poles have been damaged or destroyed, 341 transformers damaged, and more than 203 miles of power lines have been knocked down by trees, branches, or fierce winds. In addition to damaged equipment, hundreds more outages have been caused by strong winds slapping power lines together, or tree limbs falling across lines and tripping circuit−breakers. In total, since the storms began Friday, December 30, more than 1.4 million of PG&E's five million customers have been affected by power outages. More than 22,000 customers have faced power outages that have lasted 24 hours or longer.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=244646&p=22

2. *January 03, Washington Post* — **Russia increases gas flow into pipeline.** The threat of an energy crisis in Western Europe because of a dispute between Russia and Ukraine abated late Monday, January 2, after the state−controlled Russian energy giant Gazprom reversed course and decided to mostly restore the volume of gas it pumps into Ukrainian pipelines that connect to the rest of the continent. Several European countries on Monday reported sharp drops in the level of natural gas they were receiving from Russia when it ostensibly cut supplies only to Ukraine. Russian natural gas destined for Western Europe transits pipelines in Ukraine, and a reduction in the amount of gas entering the system from Russia, which was designed to affect only Ukraine, had led to reductions of up to 40 percent in supplies reaching Austria, Italy, France, Hungary, Poland and Slovakia −− all members of the European Union −− as well as Romania and Croatia. EU countries were concerned primarily with the specter of rationing or cuts of a key source of energy for industry and home heating in the depth of winter. Gazprom had cut supplies by 120 million cubic meters a day on Sunday morning, January 1.
Source: http://www.sfgate.com/cgi−bin/article.cgi?file=/chronicle/ar chive/2006/01/03/MNGFLGGIKH1.DTL

3. *January 02, Associated Press* — **Coal mine reports spate of violations.** The Tallmansville, WV, coal mine where 13 miners were trapped after an explosion Monday, January 2, was cited 208 times for alleged safety violations in 2005, up from 68 citations the year before. Federal regulators' allegations against the Sago Mine included failure to dilute coal dust, which can lead to explosions, and failure to properly operate and maintain machinery, according to the U.S. Labor Department. Ninety−six of the citations were considered "significant and substantial" by inspectors. An official with the International Coal Group, which has owned the mine since March, said the Labor Department could have closed the mine if it were deemed unsafe. "We think that we were operating a safe mine. We have no real clue about what triggered this explosion or whatever happened today," said ICG Senior Vice President Gene Kitts.
Source: http://wireservice.wired.com/wired/story.asp?section=Breakin g&storyId=1138681

4. *January 02, Christian Science Monitor* — **Energy prices cool, signal possible economic upturn.** The Katrina effect on energy prices finally appears to be fading. The price of natural gas on the futures market is down almost 30 percent from early September, when it rose sharply to reflect the damage done to scores of wells and pipelines in the Gulf of Mexico. At the same time, the price of home−heating oil has dropped almost 60 cents a gallon. And gasoline prices, which had soared to more than $3 per gallon, have now dipped to $2.15 per gallon nationally. A

major reason for the drop is that temperatures, after a cold spell earlier in December, are now almost balmy by contrast. But, it's not just lower demand. Energy supplies in the Gulf of Mexico have been slowly but steadily coming back. For example, after hurricane Katrina roared through the region, some 75 to 80 percent of natural gas production was shut−in. Today, just 19 percent of natural gas production is still out of commission. Late next month, OPEC members will meet in Vienna to look at production quotas. Already there are reports that OPEC will cut production, perhaps by as much as one million barrels of oil per day, to try to keep prices from falling.
Source: http://www.usatoday.com/money/economy/2006−01−02−economics−c sm_x.htm

5. *January 01, Reuters* — **Iran develops uranium separation machinery.** Iran said on Sunday, January 1, it had developed machinery to separate uranium from its ore, part of the state's ongoing drive to become self−sufficient in nuclear technology. The mixer−settler machinery was developed by Iran's Atomic Energy Organization, state television said. Iran's efforts to build a full nuclear fuel cycle has caused alarm in the West which fears Tehran could use the technology to build atomic weapons. Iran says it only wants to use its nuclear facilities to generate electricity. In August, Iran announced another breakthrough in nuclear technology by using biotechnology to produce larger and cheaper quantities of uranium oxide, or yellow cake, from uranium ore. Yellowcake is processed and then enriched to produce nuclear reactor fuel or, if highly enriched, bomb−grade material.
Source: http://today.reuters.com/news/newsarticle.aspx?type=worldNews&storyid=2006−01−01T144734Z_01_SCH152880_RTRUKOC_0_US−NUCLEAR−IRAN−MACHINERY.xml

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *January 03, Lawrence Journal−World (KS)* — **Hazmat concern shuts U.S. 24 in Kansas.** The reported theft of dangerous chemicals near grain elevators in Midland Junction, KS, forced local police, fire and hazardous materials responders to scramble Monday, January 2. The Douglas County, KS, Sheriff's Office shut down traffic along U.S. Highway 24 for less than a half hour on Monday afternoon while officials tested whether anhydrous ammonia −− a potentially deadly gas −− had leaked from tanks that someone had opened. The nurse tanks −− small, mobile tanks that store the fertilizer −− are often the target of methamphetamine producers, said Cristi Cain, project coordinator for the Kansas Methamphetamine Prevention Project. Although sheriff's spokesperson Lt. Kari Wempe said emergency crews found that the tanks weren't leaking, witnesses on the scene saw someone tampering with the tanks, and officers found smaller tanks for transporting the gas nearby. Although there was no gas leak Monday, Cain said that thieves often left anhydrous ammonia tanks' hoses undone, creating health and environmental hazards for farmers and those living near farms.
Source: http://www2.ljworld.com/news/2006/jan/03/hazmat_concern_shuts_us_24/?city_local

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

7. *January 03, Vnunet* — **EBay users hit by mass phishing attacks.** Online auction site eBay was the target for 96 percent of all United Kingdom phishing attacks in December, according to security specialists Fortinet. Scammers anticipated the Christmas rush to use eBay to buy presents −− and sell unwanted ones −− and are targeting eBay users in a widespread assault. Guillaume Lovet, Threat Response team leader at Fortinet, said: "One of the easiest and quickest ways to make money on the Internet is setting up an auction on eBay for a [bogus] item, cashing the money, then disappearing. However, your account is likely to be closed because of the buyer complaints. You could create a new one but people generally do not buy an expensive item from a brand new account. Hence the value of stolen eBay accounts." The company also found that one in 20 Multimedia Messaging System (MMS) messages sent via mobile phone were infected with the Commwarrior virus, suggesting that this malware may be more widespread than first thought. The virus spreads via Bluetooth between 8 a.m. and midnight, then stops these attempts and sends itself to everyone in the phone's contact lists via MMS until 7 a.m. Then it wipes all evidence of its activities.
   Source: http://www.computeractive.co.uk/vnunet/news/2147942/mass−phishing−ebay−december

8. *January 03, Wireless* — **Video exposes tools used by hackers to exploit vulnerabilities on mobile computers.** Fiberlink Communications has released a free video that details what it calls ongoing security risks and vulnerabilities that threaten mobile workers. The "Anatomy of a Hack" video shows some of the techniques, skills, and tools used by hackers to exploit vulnerabilities on mobile notebook computers in order to gain access to corporate systems. The enterprise security firm said attackers are focusing on poorly protected applications, such as the Kazaa file sharing program, Windows Media Player, and even the Firefox browser, even though it's generally considered safer than Internet Explorer. Their intent, the firm said, is to grab information that can be used to gain access to corporate systems. The 36−minute Fiberlink video mainly details how an intruder can surreptitiously take over another user's notebook with just a little knowledge and certain software tools. Once in the system, passwords and access to other corporate data are an easy next step. The intruder can also shut down an anti−spyware's ability to detect a break in.
   Video: http://www.demosondemand.com/clients/fiberlink/002/page/index_new.asp
   Source: http://www.internetnews.com/wireless/article.php/3574521

9. *January 02, Orlando Sentinel (FL)* — **Financial institutions set dubious record for identity theft.** A final flurry of computer security breaches marked the end of 2005 −− a record year for potential identity−theft activity. Almost 100 breaches were reported in 2005, including a half−dozen in December alone, according to the Privacy Rights Clearinghouse, a nonprofit watchdog group in California. Major institutions such as Bank of America and the Federal Deposit Insurance Corp. were victimized, as were little−known data−technology outfits. Computer hackers hit many colleges across the country, stealing thousands of files with account numbers and other personal data belonging to students and school employees. Other

perpetrators gained access to personal data by hijacking laptops, setting up bogus corporate accounts, or stealing passwords. Most of the biggest data thefts of 2005 involved computer−data tapes stolen as they were being shipped. Overall, almost 52 million people had their personal information put at risk as a result of data heists in 2005, the watchdog group said. Not all companies are letting their customers know when data may be compromised. Twenty−two states now require companies to notify customers of security breaches. A dozen states also have "security freeze" laws allowing potential victims of identity theft to prevent others from establishing credit in their names.
Study: http://www.privacyrights.org/ar/ChronDataBreaches.htm
Source: http://www.orlandosentinel.com/business/orl−banks0206jan02,0 ,5638345.story?coll=orl−business−headlines

10. *January 02, Computerworld* — **ABN Amro unit reveals electronic data−transfer plan after tape snafu.** ABN Amro Mortgage Group Inc. said it plans to stop sending data tapes to its credit−reporting bureaus after a tape containing personal information on more than two million customers was temporarily lost late last year. Group CEO Thomas Goldstein announced that the company has been working since last spring on a plan to encrypt data and send it over secure networks whenever possible. The project is slated to be completed this month. The plans were disclosed on Tuesday, December 19, the same day the company located the missing tape. The tape contained the names, account information, payment histories, and Social Security numbers of residential mortgage customers. Arun Taneja, founder of research firm Taneja Group Inc., estimated that only about two percent of all enterprises have taken measures such as encrypting data stored on tapes or setting up secure networks to transfer data backups. "We're basically naked as an industry when it comes to data that's encrypted or made not identifiable somehow," he said. Taneja said that over the next five years, digital tape will be used only for "deep" archive purposes, while disk−to−disk backup will be the primary means of archiving data for months or even a few years.
Source: http://www.computerworld.com/printthis/2004/0,4814,107357,00 .html

[Return to top]

Transportation and Border Security Sector

11. *January 03, WWAY 3 (NC)* — **North Carolina to build new international port on Cape Fear.** The North Carolina State Port Authority is trying to buy a 600−acre piece of land along the Cape Fear River in Brunswick County to build a new international port. The 600−acre−site is between the Town of Southport and Sunny Point Military Ocean Terminal along the Cape Fear River. According to plans, the new facility would handle two million containers a year and attract larger ships than the existing state ports just north in Wilmington and Morehead City. Port officials hope with this new port facility that they can take some of the business from ports in Norfolk, VA, and Charleston, SC. Right now the land is owned by pharmaceutical company Pfizer and they have signed a letter of intent to sell.
Source: http://www.wwaytv3.com/Global/story.asp?S=4311166&nav=menu70_2

12. *January 03, New York Times* — **A victim of the storm, I−10, enjoys a quick rebirth.** In the wake of Hurricane Katrina, the twin spans of Interstate 10 over Lake Pontchartrain were broken into pieces, their 260−ton slabs tossed into the water by the storm surge. But amid all that has

gone wrong on the Gulf Coast, the repair of the crucial highway has gone unusually right, coming in ahead of time and under budget. The State of Louisiana and the contractor were able to open one span in October and plan to have traffic flowing on the other as early as January 6, nearly two weeks ahead of schedule. With the bridges torn apart, a major artery of transportation joining New Orleans and Slidell was cut off. I−10 is one of three coast−to−coast interstates that link the entire nation, stretching from Jacksonville, FL, to Los Angeles. Road damage from Hurricanes Katrina and Rita was widespread across coastal Louisiana and Mississippi. In Congressional testimony in October, Johnny B. Bradberry, the Louisiana transportation secretary, estimated the cost of repairing and replacing the state's damaged roads, bridges, public ports, airports, railroads, and other transportation systems at $5.5 billion. But one of the highest priorities was getting the Interstate open, and doing so quickly required creative thinking, dedication, and no small amount of luck.
Source: http://www.nytimes.com/2006/01/03/national/nationalspecial/03highway.html?pagewanted=all

13. *January 03, Washington Post* — **Independence Air to end flights on Thursday.** Flyi Inc., parent of Dulles−based low−fare airline Independence Air, said on Monday, January 2, it will discontinue flights after Thursday evening, January 5, because it cannot find a buyer for its financially troubled operation. The demise of Independence Air, whose blue and white jets have become a familiar sight in the skies around Washington Dulles International Airport, will leave 2,700 employees, including 2,300 in the Dulles area, out of work, and thousands of passengers scrambling to find alternate flights and secure refunds. The shutdown also will cut competition in the 37 markets Independence serves, probably leading to higher fares at Dulles Airport. In the latest piece of bad news for the U.S. airline industry, Flyi will vanish two months after it filed for Chapter 11 bankruptcy protection, complaining of high fuel costs and intense competition, and almost 19 months after it launched service at Virginia's Dulles Airport, promising low fares and coast−to−coast service. Flyi is the largest airline to go out of business since 1991, when both Eastern Air Lines Inc. and Midway Air Lines Inc. folded, industry consultant Darryl Jenkins said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/02/AR2006010200857.html

14. *January 03, Associated Press* — **Southwest Airlines returns for opening day in Denver.** Southwest's first passenger flights in 20 years from Denver are scheduled Tuesday, January 3, with service to Las Vegas and Chicago's Midway Airport. The carrier also will offer Denver−Phoenix service, for a total of 13 daily flights. CEO Gary Kelly said Southwest will add more flights from Denver but declined to give specifics. Kelly said the time was right for Southwest to return, with lower airport fees and other favorable market conditions. Southwest will challenge Denver−based low−fare rival Frontier, which also serves Las Vegas, Chicago and Phoenix among its nearly 50 U.S. destinations. United Airlines has a hub in Denver. Frontier and United combined handle about 75 percent of the airport's passenger traffic. Southwest will probably generate an additional 1.5 million passengers a year at Denver International because it will force other airlines to reduce their fares to compete, Kelly said. Meanwhile, in Philadelphia, Southwest expanded from 14 daily flights when it launched service in May 2004 to 53 daily flights now. The airline plans to lease enough additional gates this year that it could double its flight frequency.
Source: http://www.usatoday.com/travel/flights/2006−01−03−southwest−_denver_x.htm

15. *January 03, Associated Press* — **Hainan Airlines to offer Boston−China flights.** Hainan Airlines will offer the first direct flights between Boston and China. The deal between Hainan and the Massachusetts Port Authority, which operates Logan International Airport, was announced by Mayor Thomas Menino during his fourth−term inauguration speech. It will be the first nonstop service between China and the United States for the low−cost carrier. The agreement, which still needs Federal Aviation Administration approval, calls for cargo service to begin this summer, with passenger flights to start by year's end. Hainan is China's fourth−largest airline and is in the process of changing its name to Grand China Airline.
Source: http://www.carthagepress.com/articles/2006/01/01/apindex/bus iness/d8esnrt00.txt

16. *January 03, Washington Business Journal* — **US Air offers help to Independence Air passengers.** Starting January 5, US Airways will let passengers ticketed on a canceled Independence Air flight fly standby on one of its flights for $50 each way. For $100 each way, it will give affected passengers a confirmed seat. US Airways says the $100 confirmed seat offer is good through January 31. The $50 standby offer is good through March 6. That price doesn't include a number of additional charges, like taxes, airport charges and security fees, that can take that $100 confirmed seat up to as much as $125. It's only good for travelers departing from Dulles International Airport, Reagan National Airport, and Baltimore/Washington International Airport. US Airways says the offer is only for Independence Air customers stuck with useless tickets, and only good for travel on the exact same dates.
Source: http://washington.bizjournals.com/washington/stories/2006/01 /02/daily6.html

17. *December 30, Tech Web* — **DHS to test RFID passports at San Francisco airport.** The Department of Homeland Security (DHS) will begin testing passports embedded with radio frequency identification (RFID) technology at the San Francisco International Airport mid−January, a spokesperson for the agency said Friday, December 30. Australia, New Zealand and Singapore have begun to issue passports to travelers with RFID chips. Many pass through the San Francisco, making it a likely location to test the technology, according to Anna Hinken, a US−Visit spokesperson at DHS. "We're bringing technology to the borders and chose RFID as one to help reach the goals of expediting safe entrance into the United States," she said. San Francisco is not the first major U.S. city to trial the technology. Through the US−Visit program, the DHS ran a three−month test with RFID−embedded e−passports in fall 2005 at the Los Angeles International Airport. Other RFID projects have been in the works, too. There are more trials underway. RFID chips have been embedded in I−94 forms. People who frequently cross U.S. borders to work, for example, are required to carry these forms. Tests at the five border crossings will continue through spring 2006.
Source: http://www.techweb.com/showArticle.jhtml?articleID=175800140

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

18. *January 03, Associated Press* — **South Korea, U.S. to hold talks on beef imports.** South Korea has scheduled talks with the U.S. next week on ending its two−year−old ban on American beef, the government in Seoul said Tuesday, January 3. South Korean shut its doors to U.S. beef imports in December 2003 after the first U.S. case of mad cow disease. At the time it was the third−largest foreign market for American beef, after Japan and Mexico. The two−day talks will begin Monday, January 9 in Seoul, the Agriculture and Forestry Ministry said in a release. A ministry advisory committee said last month that U.S. beef could be considered safe to consume if tougher inspection and quarantine measures were taken. The committee also said there were no decisive grounds to say U.S. beef wasn't safe. In 2002, South Korea imported 213,000 tons of U.S. beef worth $610 million, according to the U.S. Meat Export Federation.
Source: http://www.signonsandiego.com/news/world/20060103−0000−skore a−us−beef.html

19. *January 03, FoodNavigator.com* — **Foodborne infections increase.** A general increase in reported cases of campylobacteriosis over the last few years in the European Union's (EU) fifteen original member states indicates that food companies need to step up their safety procedures against the disease. The statistics are in the European Commission's first report on the persistence in the EU of a range of zoonoses, foodborne diseases, that are transmissible from animals to humans. The report takes the pulse on the state of food safety in the EU. In 2004 the 25 EU countries reported a total of 6,860 outbreaks of zoonoses, with 42,447 people affected. "The information submitted on antimicrobial resistance in zoonotic bacteria indicated that animals and food of animal origin might serve as reservoirs for resistant bacteria with the risk of direct or indirect transfer of resistant bacteria to humans," the Commission found. By far the most frequently reported zoonotic diseases in humans are salmonellosis and campylobacteriosis, with the most deadly being listerious, the report found. There were 192,703 reported cases of salmonellosis and 183,961 of campylobacteriosis cases reported during 2004 in the EU's 25 member states. The totals have increased for 2004 due to the expansion of the EU to include 10 new member states.
Source: http://www.foodnavigator.com/news/ng.asp?n=64828−food−safety −zoonoses−campylobacteria

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

20. *January 03, San Jose Mercury News (CA)* — **Bogus bird flu drugs flooding the Internet.** The Internet is awash with bogus drugs to counter a possible bird−flu pandemic, including counterfeit Tamiflu −− the highly sought−after antiviral agent. Hundreds of fake Tamiflu pills sold to U.S. consumers by Asian online entrepreneurs have been seized in San Francisco, CA, over the past month, most recently on Wednesday, December 28. How much fraudulent Tamiflu is being sold isn't clear. The manufacturer said they are aware of only one instance of counterfeit Tamiflu showing up outside the U.S. Those pills, found in Holland, contained only Vitamin C and lactose, and were improperly labeled. But government officials fear fake Tamiflu will become a growing plague, particularly in the U.S. Since November 26, U.S. Customs Service officials at the South San Francisco airmail facility say, they have seized 53 packages containing fake Tamiflu pills mailed by Asian companies to U.S. consumers who bought them online. Federal agents also confiscated a suspicious small package of Tamiflu in Honolulu on December 22, but haven't completed a chemical analysis of it. Bogus Tamiflu isn't the only worrisome bird−flu remedy being promoted on the Web. The U.S. Food and Drug Administration sent warning letters to nine Internet marketers it accused of peddling phony remedies. The companies offered everything from "soil−based organisms" to "systemic enzymes."
Source: http://www.mercurynews.com/mld/mercurynews/business/13538069 .htm

21. *January 02, Agence France−Presse* — **Strict health, security checks await Mecca pilgrims.** Saudi authorities are working hard to ensure Muslim pilgrims flocking to join the annual pilgrimage to Mecca are disease−free. "The first thing we did one month ago was compile a list of countries plagued with certain diseases," says Mohammed al−Harthi, director of the health control center at King Abdul Aziz airport in Jeddah. He says special measures have been implemented to deal with pilgrims coming from Africa, the Indian subcontinent, and countries like Egypt and Yemen where infectious diseases are common. By Friday, December 30, more than 1.1 million pilgrims had already arrived in Saudi Arabia ahead of the annual pilgrimage. It is estimated that a total of two million pilgrims will come this year. Most arrive by air. "Once a plane lands, we dispatch two inspectors," says Harthi. "The door of the aircraft is not opened until our people get there." He says inspectors collect a written certificate from the pilot confirming that the plane has been disinfected and check for empty spray canisters as proof. Passengers are then bused to a special pilgrims' terminal where they are required to produce a clean bill of health from their home country and are given supplementary vaccinations where necessary.
Source: http://news.yahoo.com/s/afp/20060102/hl_afp/saudireligionhajjhealthsecurity_060102194400;_ylt=ApI5OOTYd3Gk0r_Q8UWmqcmJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

22. *January 01, Baltimore Business Journal (MD)* — **Hospitals prepare for avian flu outbreak.** Maryland's hospitals are ramping up their emergency response plans and buying supplies in preparation for the possibility that avian influenza could strike the U.S. Public health officials worry that the H5N1 avian influenza virus, which has killed millions of birds and more than 70 people in Asia, will mutate into a form that spreads easily among humans. Maryland's hospitals in the coming months will receive seven million dollars in federal funding to help prepare for disasters, said Frank Monius, an assistant vice president with the Maryland Hospital Association. A portion of that money will pay for additional supplies of masks, facial shields,

gowns, sterile gloves, and medicine that would be needed in the event of a flu pandemic. It's a good idea for hospitals to stock up on such supplies now, Monius said, because there's likely to be a rush to buy them if there is a confirmed case in which avian flu is transmitted from one person to another. The University of Maryland, Baltimore's law school on January 13 will hold a symposium to discuss potential responses to an avian flu outbreak.
Source: http://msnbc.msn.com/id/10679972/

[Return to top]

Government Sector

23. *January 03, News−Record (NC)* — **New bailiff skilled at sniffing trouble.** There's a new bailiff patrolling the halls of Guilford County's two courthouses in Greensboro, NC. The county paid $10,000 for Brek, a two−year−old German shepherd, and an eight−week class where Deputy John Bush trained the dog. The cost includes refresher courses. Brek's first day on the job was October 31, and he has since spent his time learning the courthouse layout, as well as the county schools that he would visit if a bomb threat were made to one of them. Deputies now have nine dogs working in the Guilford County Sheriff's Department, which includes a bloodhound in training. Brek is the only dog specialized in bomb detection. Most other dogs sniff out narcotics. Sheriff's officials say they've had relatively few problems in the courthouses over the years, though Brek adds extra security. But a series of high−profile bomb threats around the Triad last spring prompted sheriff's officials to consider purchasing a bomb dog. The Greensboro Police Department uses two dogs to help hunt explosives. The city animals were in service before the bomb threats.
Source: http://www.news−record.com/apps/pbcs.dll/article?AID=/20060103/NEWSREC0101/60103001/1001/NEWSREC0201

[Return to top]

Emergency Services Sector

24. *January 03, Boston Globe* — **Blast in West Virginia mine traps 13; rescuers struggle to make contact.** Rescue workers hampered by silence, debris, and pockets of deadly carbon monoxide struggled late Monday night, January 2, to reach 13 coal miners trapped nearly 300 feet underground by a powerful mine shaft explosion in the Sago Mine of Tallmansville, WV. By nightfall, search teams had begun to move cautiously on foot down to the spot where the miners were believed to be trapped. By 10 p.m. EST, rescuers had proceeded about 4,800 feet into the shaft, still more than 8,000 feet from where the miners were believed trapped. Rescue teams were slowed, officials said, by concerns about air quality and efforts to ensure they had adequate oxygen as they descended. The teams had to wait more than 12 hours until officials drilled holes in the area above the cave−in site to vent and test for toxic carbon monoxide that they thought might have built up inside the shaft after the explosion. Rescue crews were also preparing to drill deeper borings to lower a listening device to scan for any sounds of life. And federal mine safety officials rushed a rescue robot to the cave−in site, located in a hilly rural area about 100 miles northeast of Charleston, WV.
Source: http://www.boston.com/news/nation/articles/2006/01/03/blast_

in_w_virginia_mine_traps_13/

25. *January 02, Washington Post* — **A lesson from Katrina: Pets should be considered in disaster plans.** For years, despite an estimated 69 million U.S. households with a pet, animal advocates have been relegated to the fringes of emergency planning. After Katrina, however, and the sight of people in New Orleans refusing to evacuate and in some cases dying with their pets, emergency officials are starting to take animal rescue seriously. By saving the pets, advocates said, owners can be saved as well. In Calvert and Montgomery Counties, MD, planners are trying to establish emergency pet shelters alongside those for humans. On Capitol Hill, five representatives have proposed making pet disaster planning mandatory by tying it to federal funds. Modern pet disaster planning didn't truly begin, U.S. experts said, until after Hurricane Andrew in 1992. However, Hurricane Katrina drew even more attention to the issue when the Federal Emergency Management Agency activated all four of its veterinary units, making it what the agency called the largest simultaneous deployment of veterinary relief in U.S. history −− more than 200 veterinarians. Several states, including New York and Pennsylvania, have since begun revising their evacuation plans to include pets.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/02/AR2006010200442.html

26. *January 02, Government Technology* — **Interoperability is only part of the problem plaguing emergency communication.** The 9/11 terrorist attacks triggered a nationwide scramble to develop interoperable communications among emergency responders. But Hurricane Katrina left officials scratching their heads over the utter disappearance of even basic communications. Radio system failures meant local first responders couldn't communicate easily among themselves, not to mention the array of outside agencies that arrived on the scene to help. "We didn't have an interoperability problem, we had an operability problem," said Lt. Col. Joey Booth of the Louisiana State Police. "We couldn't communicate within our own department much less with other departments. We had a lot of responders coming in to help, but our system didn't have the capacity to operate with all these new users." Experts say these shortcomings point to the need for more attention on ensuring the availability of radio systems during major disasters, or at least to creating plans that guide first responders when radio communications fail. Ultimately, the challenges of radio operability and interoperability are intertwined. To succeed, policymakers and emergency responders must tackle both issues: building radio systems that withstand worst−case disasters and linking to systems used by other agencies.
Source: http://www.govtech.net/magazine/channel_story.php/97721

27. *January 02, Travel Daily News* — **Chinese airport conducts critical anti−hijacking drill.** The first, large−scale anti−hijack drill was held at China's Guangzhou Baiyun International Airport and carried out by the newly created Guangdong Province Anti−Hijack Team. The scenario involved four mock terrorists who “hijacked” an in−flight China Southern Airlines Boeing 757 aircraft with 120 passengers on−board. They demanded the pilot fly them to another country but because the plane was “low on fuel”, it was forced to “land” at Guangzhou Baiyun International Airport. As the “hijacked” China Southern Aircraft “landed” at Baryon International Airport, the armed Anti−Hijack Team quickly besieged the runway. Two police helicopters were immediately dispatched and circled over the tarmac, while fire engines and ambulances were standing by. More than 800 law enforcement representatives from more than

10 different organizations including the Armed Police Force Corp, Guangdong Province Public Security Agency, Central and South China Air Traffic Management Bureau, General Administration of Civil Aviation of China and China Southern Airlines together with two helicopters and more than 80 automobiles joined in the mock crisis emergency simulation.
Source: http://www.traveldailynews.com/new.asp?newid=26957&subcatego ry_id=98

[Return to top]

Information Technology and Telecommunications Sector

28. *December 30, Federal Computer Weekly* — **Defense Information Systems Agency declares GIG−BE fiber net fully operational.** The Defense Information Systems Agency (DISA) declared its nationwide fiber−optic network operational Friday, December 30, but said a few outlying nodes remain to be connected in the near future. DISA's Global Information Grid−Bandwidth Expansion (GIG−BE) network consists of high−speed OC−192 circuits that connect major Department of Defense (DoD) installations in the United States. The network can handle traffic up to the top−secret level. Air Force Lt. Gen. Charles Croom, DISA's director, said GIG−BE provides DoD with "an optimized backbone similar to an interstate system where data traveling great distances can be moved at high speeds without bottlenecks." The fiber−optic network, which costs approximately $800 million, complements DISA's Defense Information Systems Network, Croom said. That network connects outlying installations and DoD activities to GIG−BE.
Source: http://www.fcw.com/article91833−12−30−05−Web

29. *December 29, Government Computer News* — **Federal agencies to spend almost $1 billion on new airwaves.** It will cost 12 federal agencies nearly $936 million to move their radio communications out of a range of the spectrum that the Federal Communications Commission (FCC) plans to auction off for next−generation mobile broadband services, according to a Commerce Department report issued last week. Under the December 2004 Commercial Spectrum Enhancement Act, which called for auctioning spectrum in the 1710− to 1755−MHz band used for fixed wireless government communications, the Commerce Department's National Telecommunications and Information Administration (NTIA) was tasked with estimating the cost of reassigning systems already operating in the band. The good news, according to NTIA, is that the $936 million figure is significantly less than wireless industry estimates. In addition to the 1710− to 1755−MHz spectrum, the FCC plans to auction spectrum in the 2110− to 2155−MHz band, which is a nongovernmental band. According to the NTIA analysis, 2,240 systems will have to be reassigned to new radio frequencies. Most of the work should be completed in three years. Affected agencies include the Defense, Energy, Homeland Security, Interior and Justice departments, as well as NASA, the Federal Aviation Administration, Internal Revenue Service and Postal Service.
Source: http://www.gcn.com/vol1_no1/daily−updates/37847−1.html

30. *January 03, Times Online (United Kingdom)* — **Nine hotspots will offer wireless Internet use in the UK.** Beginning in March, residents in nine urban centers across Britain will be able to access the Internet from their laptops outdoors, without cables, and use their mobile phones to make calls over the Web after a small technology firm launches the first part of a nationwide WiFi network. The move to roll out wireless Internet technology will threaten the revenues of

Britain’s mobile phone operators. Birmingham, Manchester and Leeds are among eight cities −− plus three London boroughs −− singled out for the installation of so−called "WiFi hotspots." Many mobile phone users will be able to bypass their mobile phone networks to make inexpensive national and international calls, send e−mails or transfer documents using the new Internet networks. Phones with a WiFi chip can link to wireless Internet networks at the touch of a button. There are at present about 25 mobile phone handsets that have WiFi chips installed. However, that number is set to increase rapidly as the technology becomes more widely available.
Source: http://business.timesonline.co.uk/article/0,,9075−1967322,00 .html

31. *January 02, IDG News Service* — **SANS: Don't wait for Microsoft to fix WMF flaw.** Windows users should install an unofficial security patch now, without waiting for Microsoft to make its move, advised security researchers at the SANS Institute's Internet Storm Center (ISC). Their recommendation follows a new wave of attacks on a flaw in the way versions of Windows from 98 through XP handle malicious files in the WMF (Windows Metafile) format. One such attack arrives in an e−mail message entitled "happy new year," bearing a malicious file attachment called "HappyNewYear.jpg" that is really a disguised WMF file, security research companies, including iDefense and F−Secure, said Sunday, January 1. Even though the file is labeled as a JPEG, Windows recognizes the content as a WMF and attempts to execute the code it contains. Staff at the ISC worked over the weekend to validate and improve an unofficial patch developed by Ilfak Guilfanov to fix the WMF problem, according to an entry in the Handler's Diary, a running commentary on major IT security problems on the ISC Website.
Updated version of Guilfanov's patch: http://isc.sans.org/diary.php?storyid=999
Source: http://www.techworld.com/security/news/index.cfm?NewsID=5070 &inkc=0

32. *January 02, eWeek* — **Sprint to acquire Velocita Wireless.** In an acquisition announcement, Sprint Nextel said it will buy Velocita Wireless, a wireless data service company that provides e−mail, messaging, vehicle location, point−of−sale and other services to about 400,000 enterprise and government customers. The acquisition brings Sprint Nextel much−needed spectrum in the 900MHz band to fill in gaps in the IDEN Walkie−Talkie−like network built by Nextel through dozens of acquisitions of small, mobile radio operators.
Source: http://www.eweek.com/article2/0,1895,1907190,00.asp

33. *January 01, Security Focus* — **IBM AIX getShell and getCommand file enumeration vulnerability.** IBM AIX is prone to a local vulnerability in getShell and getCommand. This issue may let local attackers enumerate the existence of files on the computer that they wouldn't ordinarily be able to see.
Source: http://www.securityfocus.com/bid/16102/info

34. *January 01, Security Focus* — **IBM AIX getShell and getCommand partial file disclosure vulnerability.** IBM AIX is prone to a local vulnerability in getShell and getCommand. This vulnerability may let the attacker gain unauthorized read access to shell scripts on the computer.
Source: http://www.securityfocus.com/bid/16103/info

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of active exploitation of a vulnerability in how Microsoft Windows handles Windows Metafiles (".wmf"). Several variations of the WMF exploit file have been released that attempt to avoid detection by anti−virus software and intrusion detection and intrusion prevention systems. A Windows system may be compromised through several methods including:

Opening a specially crafted WMF file. Note that a malicious WMF file may masquerade as a JPEG or other type of image file.

Visiting a specially crafted web site.

Placing a malicious WMF file in a location that is indexed by Google Desktop Search or other content indexing software.

Viewing a folder that contains a malicious WMF file with Windows Explorer.

Once the vulnerability is exploited, a remote attacker may be able to perform any of the following malicious activities:

Execute arbitrary code

Cause a denial of service condition

Take complete control of a vulnerable system

For more information about this vulnerability please review:

Technical Cyber Security Alert TA05−362A / Microsoft Windows Metafile Handling Buffer Overflow:

http://www.us−cert.gov/cas/techalerts/TA05−362A.html

US−CERT Vulnerability Note VU#181038 / Microsoft Windows Metafile handler SETABORTPROC GDI Escape vulnerability:

http://www.kb.cert.org/vuls/id/181038

Microsoft Security Advisory 912840 / Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution

http://www.microsoft.com/technet/security/advisory/912840.ms px

Although there is limited information on how to fully defend against this exploit, US−CERT recommends the following mitigation:

Unregister SHIMGVW.DLL

Please see VU#181038 at URL http://www.kb.cert.org/vuls/id/181038 for details and additional workarounds.

We will continue to update current activity as more information becomes available.

RIM BlackBerry Vulnerabilities US−CERT information about multiple vulnerabilities in RIM BlackBerry products has been presented at the 22nd Chaos Communication Congress. The vulnerabilities could allow an attacker to execute arbitrary code on or cause a denial of service to the BlackBerry Attachment Service. An attacker could also cause a denial of service to the BlackBerry Router or the web browser on BlackBerry Handheld devices. To exploit these vulnerabilities, an attacker would need to supply a crafted file that is viewed or downloaded by a BlackBerry Handheld; or the attacker would need redirect a network connection directed to the BlackBerry Infrastructure.

US−CERT recommends that BlackBerry sites upgrade BlackBerry Enterprise Server to the latest version and consult the BlackBerry Technical Knowledge Center at URL:

http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/customview.html?func=llworkspace

For further details please see the following URL:

http://www.kb.cert.org/vuls/id/829400

http://www.kb.cert.org/vuls/id/392920

http://www.kb.cert.org/vuls/id/570768

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 80 (www), 27015 (halflife), 42011 (−−−), 6888 (muse), 6999 (iatp−normalpri), 1025 (win−rpc), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: 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]

Commercial Facilities/Real Estate, Monument &Icons Sector

35. *January 03, WXYZ (MI)* — **Heightened security on the Detroit People Mover.** Over the next four weeks, Detroit will host two international events, the Auto Show and the Super Bowl. This will mean stepped up security everywhere, and the city is taking extra precautions with the People Mover. The city of Detroit says visitors to the city who are planning on riding the People Mover while downtown for the Auto Show and up through the Super Bowl, should not carry a backpack or large package. Random security checks will be made, and people carrying big bags could be delayed for some time. According to Al Fields, of the Detroit Transportation Corporation, "We are going to be surveying things and looking for suspicious packages. [Purses and briefcases could also fall into those categories.] Anything that could hold something that we don't want on the system." City officials say the heightened security will be in effect from January 8th, all the way through the Super Bowl on February 5th.
For more information, visit the Detroit People Mover Website:
http://www.thepeoplemover.com/Home.id.2.htm
Source: http://www.wxyz.com/wxyz/nw_local_news/article/0,2132,WXYZ_15924_4359781,00.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure 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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

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