Department of Homeland Security Daily Open Source Infrastructure Report for 05 January 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The National Public Radio reports increased coal demand has caused the mining industry to go from a stagnant to a growth industry within a few years, and the disaster at West Virginia's Sago Mine has raised new questions about coal mining safety. (See item 2)
- The Associated Press reports about 200 United Airlines flights worldwide were delayed up to 90 minutes Tuesday, January 3, because of a glitch in the computer system controlling check−ins and reservations. (See item 10)
- The Department of Homeland Security has announced $765 million in direct funding to provide resources for the unique equipment, training, planning, and exercise needs of select high threat urban areas, as part of the Urban Areas Security Initiative. (See item 24)

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 04, Reuters* — **Pipeline blasts shut down U.S.−owned power plant in Pakistan.** Suspected tribal rebels blew up a gas pipeline in Pakistan's troubled province of Baluchistan early on Wednesday, January 4, shutting down supplies to a U.S. and British−owned power plant, police and company officials said. Two blasts damaged a 24−inch diameter pipeline at

two places in the Dera Murad Jamali area, about 140 miles southeast of the provincial capital Quetta, cutting off the gas supply to the nearby Uch private power plant. "It is an act of sabotage. There were two big explosions," said district police officer Naseebullah Ghilzai. A spokesperson for the 586−megawatt Uch power plant, Tariq Jamali, said the blasts had damaged two sections of pipeline, one about 10 feet long and the other about eight feet long. He said the plant would remain closed until the pipeline, which is not owned by the power plant, was repaired, but he could not say how long this would take. The main shareholders of the Uch plant are Britain's International Power Plc, and U.S. firms Tenaska Inc and GE Capital. It sells electricity to Pakistan's state−run Water and Power Development Authority, which said there had been no disruption to electricity supplies.
Source: http://asia.news.yahoo.com/060104/3/2de5d.html

2. *January 04, National Public Radio* — **Mining accident raises broader safety questions.** This week's mining disaster at the Sago Mine in Tallmansville, WV, has raised new questions about coal mining safety. Since 2000, increased demand for coal and other mined materials, a shortage of skilled miners, and the reopening of some older mines with aging equipment has contributed to more than 300 fatalities. However, according to Davitt McAteer, former assistant secretary for mine safety and health for the Department of Labor, mining safety in the U.S. has improved dramatically since passage of the Mining Safety and Health Act of 1997. In 1997, 272 miners died on the job, versus 56 in 2003. Mine explosions aren't all that common, he says. Typical incidents include roof collapses, electrocution, and safety problems associated with haulage and transportation. Underground miners are required to carry Self−Contained Self−Rescuer (SCSR) units. The National Institute of Occupational Safety and Health is developing a next−generation SCSR system that's smaller and lasts longer. Technology improvements have dramatically improved productivity, allowing one man to produce 13 tons of coal per day today, versus three tons in the 1970s. Increased coal demand (mostly to power electric utilities), has caused the industry to go from a stagnant to a growth industry within a few years.
Source: http://www.npr.org/templates/story/story.php?storyId=5125860

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

3. *January 03, Rand Corporation* — **A new direction for China’s defense industry.** Over the past 25 years, U.S. research has concluded that China’s defense−industrial complex is rife with weaknesses and limitations. A new study by the Rand Corporation states that it is time to acknowledge gradual improvements in China’s defense industry, certain sectors of which are producing a wide range of increasingly advanced weapon systems that will enhance China’s military capabilities. Rand’s research suggests that revitalization of China’s defense sector, and reform, have accelerated over the past five years. These moves have allowed China’s defense

industry to emerge from the doldrums of two and a half decades of systemic neglect, inefficiency, and corruption. Improvements in China's defense research, design, and production capabilities have been uneven across sectors. The missile sector has progressed at an accelerated pace over the past five years, suggesting that China may soon begin fielding land−attack cruise missiles, higher−quality anti−ship cruise missiles, modern long−range surface−to−air missiles, and anti−radiation missiles. The shipbuilding industry has gradually modernized, resulting in increasingly sophisticated platforms and heightened production rates. The aviation industry, which has been inefficient in the past, is showing signs of limited progress; but important gaps in design and production capabilities remain.
Rand study: http://www.rand.org/pubs/monographs/2005/RAND_MG334.pdf
Source: http://www.defense−aerospace.com/cgi−bin/client/modele.pl?session=dae.17036408.1136395209.Q7wDycOa9dUAAAFO6kw&modele=jdc _34

4. *January 03, Associated Press* — **Congress drops "Buy America" for tankers.** A defense bill approved by Congress would allow open competition for a multibillion−dollar contract to supply refueling tankers for the Air Force. President Bush is expected to sign the measure, squelching an earlier House−approved bill that would have helped the Boeing Co. by keeping the Pentagon from buying military equipment from the parent company of European jet maker Airbus SAS. "Buy America" language had been inserted by Rep. Duncan Hunter (R−CA) chairman of the House Armed Services Committee. However, Hunter agreed to remove the provision last month at the request of Senate leaders and administration officials, who said it could spark retaliatory measures by other countries and limit Pentagon flexibility. Congress voted final passage December 21. George Behan, chief of staff to Rep. Norm Dicks, D−WA, said withdrawal of the buy−America clause was expected. "There's no question there will be an open competition. The real question is whether the Pentagon will ever award the contract to a company that has a major European component, given the [U.S.] complaints about illegal subsidies the parent company is receiving," Behan said. The House bill would have barred the Pentagon from purchasing goods and services from foreign companies that receive government subsidies.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/03/AR2006010300992.html?sub=AR

[Return to top]

Banking and Finance Sector

5. *January 03, WISC−TV Channel 3000 (WI)* — **Wisconsin legislators propose measure to avert identification theft.** Wisconsin Attorney General Peg Lautenschlager and Senator Russ Decker (D−WI) are supporting a bill that seeks to offer residents greater protection from identity theft. The proposed bill would give Wisconsinites control over their credit report by allowing them to freeze it, meaning no one else could access it without permission. The measure would also make it illegal for a business to discriminate against anyone simply because they won't provide their Social Security number. The bill also increases the penalties for criminals of mail theft −− to up to three years in prison and a $10,000 fine. About 12 other states already have a similar law. Identity theft is the fastest−growing, white−collar crime in the country. In 2004, about 2,646 people in the state were victims. Lautenschlager said, "We have identity theft laws on the books which are good ones, frankly...They are better than many states

have but we would like to get those better and we would like to make those stronger in terms of the consequences that are attached to the crimes of identity theft." The bill's supporters are also looking at perhaps fining companies that lose people's information and make them susceptible to ID theft.
Source: http://www.channel3000.com/news/5825780/detail.html?rss=c3k& psp=news

6. *January 03, NBC−2 News (FL)* — **Perpetrators charged in unusual bank scam.** A Southwest Florida couple is under arrest and their 21−year−old daughter is on the run after an unusual method to steal money from a Punta Gorda, FL, bank. Police say they've never seen anything like it −− and the alleged thieves weren't very hard to find. The case involved an ATM machine at a Suncoast schools credit union branch. It was a relatively simple scam. Police say the family deposited empty envelopes into the machine then withdrew money supposedly covered by the amount of the deposit. The entire affair, including three different trips to the ATM to pull off the scam, was captured on surveillance video. "It was pretty easy for us to track them down. Obviously, you start with your account holder and just go from there. Certainly this was not the brightest thing for them to do," said Punta Gorda Police Department spokesperson Jason Ciaschini. Most banks don't allow customers to withdraw money in the manner used by the alleged thieves.
Source: http://www.nbc−2.com/articles/readarticle.asp?articleid=5386 &z=3&p=

7. *January 03, Buffalo News (NY)* — **New York state warns about scam to get codes for credit cards.** The state Banking Department has issued a warning to consumers to watch out for scams designed to get them to reveal the three−digit security number on the back of credit cards. The scam occurs when someone who claims to be from the security or fraud department of a major credit card company calls a consumer and provides a phony badge number. The person already has the consumer's credit card number, having obtained it illegally from another source, and claims the consumer's card was noted for an "unusual purchase pattern" for a recent purchase under $500. The caller reassures the consumer that a credit will appear on the next billing statement, and provides a phony control or confirmation number to "document" the fraud. The caller then asks the consumer for the three−digit security number, allegedly to prove the consumer has the card in hand. Once the thieves have the three−digit security number, along with the credit card number, there's nothing to prevent fraud. Within 15 minutes, the thieves will usually make a purchase in the amount he or she told the consumer was flagged. Having been warned, the consumer won't find it unusual, and won't suspect anything until it's too late.
Source: http://www.buffalonews.com/editorial/20060103/1054964.asp

8. *January 03, CNET News* — **H&R Block blunder exposes consumer data.** Some consumers may be dismayed to find their Social Security numbers printed on unsolicited packages from H&R Block, the result of a recent labeling blunder at the company. The packages, which H&R Block mailed in December, contained free copies of the company's tax preparation software, TaxCut. By mistake, some of the packages also displayed recipients' Social Security numbers, which were embedded in 47−digit tracking codes above mailing labels. The company informed affected customers of the error via letters sent on Thursday, December 22, and on its Website. H&R Block said the risk of identity theft based on the incident is low because the Social Security numbers are hidden in a string of characters and aren't formatted like Social Security numbers with dashes between numbers. The number of people affected by the problem is unclear. H&R Block spokesperson Denise Sposato said it's less than three percent of the people

who received the packages. She declined to specify how many people overall were included in the mailing. Sposato said the incident was a result of human error and that the company is reviewing its procedures to ensure it doesn't happen again. No data has been lost or stolen as a result.
Source: http://news.com.com/H38R+Block+blunder+exposes+consumer+data/2100−1029_3−6016720.html?tag=cd.top

9. *January 03, TechWeb News* — **South Korea, Romania, Russia host high percentage of phishing URLs.** Of more than 41,000 phishing URLs that Netcraft −− a U.K−based Web performance and anti−phishing firm −− confirmed in 2005, 62 percent targeted eBay and PayPal. Many were what Netcraft dubbed "insta−spoofs," bogus URLs hosted from free sites or compromised machines, the latter often via a botnet. According to Netcraft, "Many of these spoof sites bear identical structures and file titles, suggesting deployment via kits that can be rapidly unpacked on a new machine." The report added that eBay and PayPal have more than 68 million active users between them, which is particularly attractive to phishers because bulk phishing e−mails will get a higher percentage of "hits" than other potential financial targets. Netcraft also reviewed a 5,000−site sample of phishing URLs to find their country of origin, and tagged Romania and Russia as the only nations whose top−level domains accounted for more than one percent of the year's phishing sites. (The bulk used the generic .com top−level domain.) Romania, in fact, hosted 1,397 phishing sites in 2005, or about three percent of all .ro hostnames. Only South Korea hosts a higher percentage of phishing URLs (3,807 phishing URLs, or around nine percent of all sites with the .kr domain).
Source: http://www.techweb.com/wire/security/175800738;jsessionid=HCQOZBHQGSYK0QSNDBCSKHSCJUMEKJVN

[Return to top]

Transportation and Border Security Sector

10. *January 04, Associated Press* — **Computer glitch delays United Airlines flights.** About 200 United Airlines flights worldwide were delayed up to 90 minutes Tuesday, January 3, because of a computer glitch. The airline's computer system controlling check−ins and reservations went down around 5 p.m. CST Tuesday, airline spokesperson Jean Medina said. The system was fixed about four hours later but caused about 200 flights to be delayed as airports had to check in passengers manually, spokesperson Jeff Green said. Medina said flights were delayed 60 to 90 minutes because of the problem. Some flights pushed back their takeoff times to allow passengers stuck in long lines to board, while other passengers had to reschedule flights, she said.
Source: http://www.usatoday.com/travel/news/2006−01−04−united−flight −delays_x.htm

11. *January 04, WABC (NY)* — **Commuter jet evacuated at LaGuardia.** There were some tense moments aboard a commuter jet at LaGuardia Airport on Tuesday, January 3, after smoke appeared in the cockpit and the flight was evacuated. The Port Authority told Eyewitness News that 17 people aboard a Colgan Airways plane were evacuated when smoke appeared in the cockpit. It happened just before 1:30 p.m. EST. No injuries were reported and the source of the smoke was not immediately known. No fire was found aboard the plane but the aircraft was taken back to the hangar and the passengers went back to the terminal.

Source: http://abclocal.go.com/wabc/story?section=local&id=3778268

12. *January 04, Associated Press* — **Couple sues over missing ring at Logan Airport.** A Rhode Island man has sued the federal government alleging his $7,000 wedding ring was stolen as he passed through the security checkpoint at Boston's Logan International Airport. John Wright, 51, of Tiverton, RI, says he and his wife were taking a flight to San Juan, Puerto Rico, in July when he placed the 1.53−carat diamond and gold ring in a plastic tub, along with his Rolex watch and wallet. He then placed the bin on the conveyer belt as he and his wife, Janet, passed through the metal detector. When he retrieved his belongings, Wright said, the ring was missing. He alerted the three Transportation Security Administration (TSA) screeners who were at the checkpoint, and they searched the conveyer belt, without success. He said he suspects one of the TSA screeners took the ring because there were no passengers in front of him as he went through the checkpoint with his wife, who was directly behind him. Ann Davis, a spokesperson for TSA, said she could not comment on the case, but said the agency does not tolerate workplace theft and aggressively investigates all complaints.
Source: http://www.usatoday.com/travel/news/2006−01−04−tsa−wedding−r ing_x.htm

13. *January 04, Reuters* — **United Airlines to emerge stronger from bankruptcy, analysts.** United Airlines' parent, UAL, perhaps just weeks from ending a three−year stay in bankruptcy, is poised to emerge strong, but analysts warn that fuel costs and a high debt load still present high hurdles for the No. 2 U.S. carrier. UAL last week got the green light from creditors to proceed with a reorganization plan. The plan still needs court approval and airline managers must address lingering objections. Nevertheless, analysts are confident that United will indeed leave court protection in February after missing previous timetables for exit. "It looks like the last hurdles are something they can get over here," said Bill Warlick, an analyst at Fitch Ratings. He noted, however, that United is set to emerge only with the aid of $3 billion in exit financing, which represents a big claim on the company's cash flow. United and the airline industry remain under pressure as they face soaring fuel prices and low−fare competition that makes it difficult for airlines to pass their expenses on to customers. Some analysts see good things ahead for United, which used its time in bankruptcy to cut costs by $7 billion, restructure contracts with its United Express unit, and dump its under−funded pensions.
Source: http://www.usatoday.com/travel/news/2006−01−04−united_x.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

14. *January 04, Agricultural Research Service* — **New sugarcane variety resists major diseases.** Sugarcane growers in Florida are quickly adopting a new variety that has shown resistance to the major yield−limiting diseases common there. Developed by scientists with the Agricultural Research Service (ARS), the University of Florida, and the sugarcane industry, the new variety

is known as CP 89−2143 and has a high sugar content from October through March −− roughly the entire sugarcane harvest season. As the nation's largest producer of sugarcane and sugar, Florida fills more than 22 percent of the nation's domestic sugar needs. The sugar industry in Florida processes two million tons of raw and refined sugar each year, adding more than two billion dollars to the state's economy. CP 89−2143's acreage has increased quickly, from just one percent of sugarcane acreage in the state in 2000 to 14.9 percent in 2004. It is expected that updated figures will show CP 89−2143 to easily exceed 15 percent of Florida's total sugar cane acreage.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

[Return to top]

Food Sector

15. *January 04, Bangkok Post (Thailand)* — **Thailand lifts import ban on U.S. beef.** The Thai government has decided to lift its ban on beef imports from the U.S., the official Thai News Agency reported Wednesday, January 4. The lifting of the ban is on condition that U.S. authorities certify in writing that every shipment is free from bovine spongiform encephalopathy (BSE). Deputy Prime Minister and Commerce Minister Somkid Jatusripitak told journalists this afternoon that the decision was made after a meeting of all agencies concerning food safety, including those under the Ministries of Public Health and Agriculture and Cooperatives. The two−year ban will be lifted next week when U.S. and Thai officials in charge of food safety meet on Monday, January 9. Thailand imposed a total ban on imported U.S. beef in late 2003 after a case of BSE was confirmed in Washington state.
Source: http://www.bangkokpost.com/breaking_news/breakingnews.php?id =70998

[Return to top]

Water Sector

16. *January 04, San Diego Union−Tribune (CA)* — **Escondido fined $1.8 million over water treatment.** A California state water board has fined the city of Escondido $1.8 million for numerous water−quality violations at its Hale Avenue sewage treatment plant. In a letter dated December 30, the state Regional Water Quality Control Board accused the city of a laundry list of violations at the plant. They range from a 354,000−gallon spill into Escondido Creek that affected the San Elijo Lagoon in Encinitas to 47 occurrences of overflows of wastewater from the plant between January and March of last year. The board also penalized the city for failing to meet deadlines for completing compliance reports. Under one violation, the city allegedly did not submit status reports on its water−reclamation program for seven years. The fines include a $1.2 million penalty the board imposed in 2004 for nearly 400 sewage−treatment violations over a period of weeks because of a failure of the treatment process used by the city plant.
Source: http://www.signonsandiego.com/news/northcounty/20060104−9999 −1mi4efines.html

17. *December 30, U.S. Environmental Protection Agency* — **Funds targeted for water quality monitoring.** The U.S. Environmental Protection Agency (EPA) has announced its plans to allocate the FY 2006 increase of $18 million for national water quality monitoring. These funds

supplement an existing allocation of approximately $200 million annually to support state, interstate agency, and tribal programs to combat water pollution. The EPA is changing the way it allocates funds under the water pollution control grant program (known as Section 106 of the Clean Water Act). The EPA allocates the funds through a prescribed allotment formula. Under the revised process, EPA will be better able to target these additional funds to help carry out priority areas that include monitoring for pollutants. The process requires the EPA to consult with states and interstate agencies prior to finalizing the allocation formula.
Source: http://yosemite.epa.gov/opa/admpress.nsf/27166bca9a9490ee852570180055e350/ad4e6d4dbec7bf3d852570e70061e514!OpenDocument

[Return to top]

Public Health Sector

18. *January 04, Agence France−Presse* — **China confirms bird flu in third−most populous province.** China has suffered its first bird flu outbreak in southwestern Sichuan, the nation's third−most populous province and a major agricultural base. A disease that killed 1,800 birds in a village in Dazhu county in the southwest Chinese province in late December was confirmed as the H5N1 virus Tuesday, January 3, the agriculture ministry said. Nationwide, it was the 32nd outbreak among poultry since early 2005. Twenty−eight of the outbreaks have occurred within the past three months, raising fears that China is facing the risk of a nationwide epidemic among its poultry industry, the biggest in the world. China has confirmed seven human cases of bird flu since late last year, including three fatalities, with the latest −− the death of a 41−year−old woman −− announced last week. Sichuan, with more than 87 million inhabitants, has traditionally been one of the country's main agricultural production areas.
Source: http://news.yahoo.com/s/afp/20060104/hl_afp/healthchinaflu_0 60104082803

19. *January 04, Associated Press* — **Minnesota nurse gets nine months for flu shot scam.** A nurse who staged a flu clinic using diluted vaccine on a college campus was sentenced Wednesday, January 4, to nine months in federal prison. Michelle Torgerson apologized for giving watered−down shots to more than three−dozen students and faculty members. Health officials said the shots weren't dangerous, nor were they strong enough to ward off the flu. Sentencing guidelines called for a prison term of between six and 12 months. A year ago, Torgerson created a scare at Augsburg College in Minneapolis, MN, after putting on a $20−a−shot clinic and fleeing when school officials confronted her about being there. In May, Torgerson, 34, pleaded guilty to a felony charge of dispensing a drug without a prescription. Four other charges were dropped in exchange for her guilty plea. In the plea, Torgerson admitted to thinning flu vaccine with saline to increase the quantity of her supply. The indictment said she pocketed about $580 in cash from the phony clinic.
Source: http://www.usatoday.com/news/health/2006−01−04−phony−flu−sho ts_x.htm

20. *January 03, Detroit News (MI)* — **West Nile cases, deaths climb.** As of September 1, 2005, there were just four confirmed human cases of West Nile virus in Michigan, but that number grew to 62 by the end of the mosquito season. Four of the people died. The late jump made brought the number of infections and deaths to their highest number since 2002.The numbers had been falling prior to last year. Michigan had 16 reported cases and no deaths in 2004, and 19 cases with two deaths in 2003. The increase is blamed on the dry summer and high

concentration of infected mosquitoes in populated areas, said T.J. Bucholz, a spokesperson for the state health department. "There was a higher population of infected mosquitoes in more populated areas like Oakland and Wayne counties," he said Monday, January 2. Michigan isn't the only state dealing with the virus. Forty−two states reported human cases in 2005, according to the U.S. Centers for Disease Control and Prevention. Arizona, Texas, and Louisiana each had more than 100 cases while Illinois had nearly 250 and California had 865.
West Nile virus information: http://www.cdc.gov/ncidod/dvbid/westnile/index.htm
Source: http://www.detnews.com/apps/pbcs.dll/article?AID=/20060103/LIFESTYLE03/601030351/1040

21. *January 02, Scripps Howard News Service* — **Treating strep throat the old way isn't working anymore.** When it comes to treating strep throat, older types of antibiotics are increasingly less likely to kill the germ that causes millions of sore throats and fevers each year. Yet recent studies show that as many as 90 percent of children treated for strep still get amoxicillin or penicillin rather than newer antibiotics known as cephalosporins. One study presented at a recent scientific meeting on antimicrobials found that taking the newer drugs even for a few days is more effective against strep than the traditional 10−day course of the older antibiotics. Pediatricians at the University of Rochester Medical Center found that 25 percent of children treated for strep with penicillin ended up back in the doctor's office within three weeks of treatment. Children treated with amoxicillin returned 18 percent of the time. But repeat visits fell to 14 percent for youngsters who got older−generation cephalosporins, and to just seven percent for newer types of the drugs, such as cefpodoxme and cefdinir, which can typically be given for just four or five days.
Source: http://www.sitnews.us/0106news/010206/010206_shns_strepdrugs_.html

[Return to top]

Government Sector

22. *January 04, Associated Press* — **City hall in Montana evacuated due to detected carbon monoxide.** The City Hall was evacuated Tuesday after utility workers found "extremely high levels" of carbon monoxide in the building, a Miles City Fire Department captain said. The evacuation occurred soon after new members of the City Council took their oaths of office at 9 a.m. MST. The building reopened in the afternoon. "What was amazing was when we went in, there was a faint smell, but when we came out, it would just about knock you down," said Mayor Butch Grenz. Fire Capt. Kevin Quinlan said he and two other firefighters were called to ventilate the building, because workers for Montana−Dakota Utilities had detected high levels of carbon monoxide. According to Quinlan's report, employees of the utility and a plumbing firm checked the furnace and water heater, and determined a fresh−air vent was almost covered. Carbon monoxide from the boiler exhaust was drawn back into the building.
Source: http://www.helenair.com/articles/2006/01/04/helena/a07010406_04.txt

[Return to top]

Emergency Services Sector

23. *January 03, Federal Computer Weekly* — **Federal Communications Commission interested in emergency wireless network.** The Federal Communications Commission (FCC) will study the feasibility of constructing a nationwide interoperable wireless network for emergency workers using some of the spectrum that TV companies will abandon as they transition to digital television. Providing mobile broadband communications, in addition to upgraded communications equipment and training, could offer emergency responders many important capabilities, the FCC said in a recent report to Congress. Although commercial providers naturally favor the use of commercial technologies and providers for at least parts of the network, some comments to the FCC by public safety entities indicate the opposite should be the case. The Arizona Regional Review Committee, for example, said that although the lack of suitable spectrum has forced many public safety entities to use commercial services, in most cases, they don't provide the backup power, site security and redundancy that a dedicated, closed system would. The Milwaukee Police Department said commercial wireless service "does not provide the reliability, features and flexibility [necessary] for critical internal communications." Given the needs of public safety, the FCC said it would act expeditiously to determine if some spectrum in the 700 MHz band could be modified for broadband wireless communications.
Source: http://www.fcw.com/article91846−01−03−06−Web

24. *January 03, Department of Homeland Security* — **Department of Homeland Security introduces risk−based formula for Urban Areas Security Initiative grants.** The Department of Homeland Security (DHS) announced Tuesday, January 3, $765 million in direct funding for high threat urban areas as part of the fiscal year 2006 Urban Areas Security Initiative (UASI). UASI provides resources for the unique equipment, training, planning, and exercise needs of select high threat urban areas. "The department is investing federal funding into our communities facing the greatest risk and demonstrating the greatest need in order to receive the highest return in our nation's security," said Homeland Security Secretary Michael Chertoff. In fiscal year 2006, the department identified 35 areas eligible to apply for and receive funding. These 35 areas encompass 95 cities with populations of 100,000 or more. The fiscal year 2006 UASI list of eligible applicants and recipients is determined through a robust risk formula that considers three primary variables: consequence, vulnerability, and threat. Factors such as the presence of international borders, population and population density, the location of critical infrastructure, formal mutual aid cooperation, law enforcement investigations and enforcement activity are considered in correlation with the risk formula for UASI determinations.
List of FY06 UASI Eligible Applicants:
http://www.dhs.gov/interweb/assetlibrary/FY06_UASI_Eligibili ty_List.pdf
Remarks by Homeland Security Secretary Michael Chertoff on the UASI grants:
http://www.dhs.gov/dhspublic/display?content=5319
Source: http://www.dhs.gov/dhspublic/display?content=5317

25. *January 03, University of Arkansas for Medical Sciences* — **National study shows many schools unprepared for disaster.** A national study conducted by the University of Arkansas for Medical Sciences (UAMS) and Arkansas Children's Hospital Research Institute (ACHRI) has shown that many public school districts have important deficiencies in their emergency and disaster plans. The results of "Mass Casualty Events at School: A National Preparedness Survey" was published in the Tuesday, January 3, issue of Pediatrics, the official journal of the American Academy of Pediatrics. The object of the study was to document the preparedness of

public schools in the United States for the prevention of and response to a mass casualty event. The study included a random survey of 3,670 school superintendents throughout the country. While 86.3 percent of respondents reported having a mass casualty response plan, only 57.2 percent have a written plan for prevention of such an event. Most school districts (66.2 percent) do not use any form of student identification such as badges or cards. Almost half (48.5 percent) do not require staff or teacher identification, and 30 percent have never conducted an emergency drill. Overall, the study concluded that personnel at urban schools are better prepared in almost all areas to handle a mass casualty emergency than those at rural schools. The study will soon be available for purchase online: http://pediatrics.aappublications.org/
Source: http://www.uams.edu/update/absolutenm/templates/news2003v2.asp?articleid=4366&zoneid=18

[Return to top]

Information Technology and Telecommunications Sector

26. *January 03, Security Focus* — **Intel Graphics Accelerator driver remote denial of service vulnerability.** The Intel Graphics Accelerator driver is susceptible to a remote denial of service vulnerability. This issue is demonstrated to occur when the affected driver attempts to display an overly long text in a text area. This allows attackers to crash the display manager on Microsoft Windows XP, or cause a complete system crash on computers running Microsoft Windows 2000. Other operating systems where the affected display driver is available are also likely affected.
Source: http://www.securityfocus.com/bid/16127/references

27. *January 03, Security Focus* — **Microsoft Windows graphics rendering engine WMF SetAbortProc code execution vulnerability.** Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability. The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. The issue may be exploited remotely or by a local attacker. Any remote code execution that occurs will be with the privileges of the user viewing a malicious image. An attacker may gain SYSTEM privileges if an administrator views the malicious file. Solution: Microsoft has released a security advisory (Microsoft Security Advisory 912840) confirming this issue. The advisory contains information about workarounds. Microsoft plans to release updates to address this issue on Tuesday, January 10.
Microsoft Security Advisory 912840:
http://www.microsoft.com/technet/security/advisory/912840.ms px
Source: http://www.securityfocus.com/bid/16074/references

28. *January 03, Tech Web* — **December instant messaging attacks jump 826 percent over 2004.** Attacks against public instant messaging (IM) networks soared over 800 percent in December 2005, compared to the same month last year, a security company announced Tuesday, January 3. According to IMlogic's Threat Center, December 2005's instant message exploits jumped 826 percent over December 2004, just the latest proof of the expanding threat facing IM users throughout the year. December, however, was slightly off the previous two months. The year's last month saw 241 new threats, said IMlogic, down from the 307 in November and the 294 in October. Combined, the three months showed a 13 percent increase in IM threats over the third

quarter of 2005. IM attacks not only continue to grow in number, but also keep gaining in sophistication, said IMlogic chief technology officer Jon Sakoda. MSN was the most heavily−hit IM network in December, added IMlogic, and accounted for 48 percent of the total threats launched. America Online's AIM, meanwhile, tallied 41 percent, while Yahoo's instant messaging network came in a very distant third, with 11 percent.
IMlogic year−end results of its IM tracking effort:
http://www.imlogic.com/im_threat_center/index.asp
Source: http://www.securitypipeline.com/news/175800842

29. *January 03, Information Week* — **Hackers find security hole in BlackBerry enterprise server.** Research In Motion's (RIM) BlackBerry Enterprise Server product may be vulnerable to denial of service attacks, according to a group of German hackers, called Phenoelit, that identifies security flaws. Phenoelit found a problem in the way the server's BlackBerry Router handles Server Routing Protocol packets. An attacker could cause denial of service by sending "specially crafted" packets to the router, according to the U.S. Computer Emergency Readiness Team. The result could be disrupted communications between the BlackBerry Enterprise Server and BlackBerry devices. In a prepared statement, Research In Motion said it "has already developed software fixes for the issues identified by [the group] and although there have been no customer reports of any actual problems, RIM has also provided temporary precautionary measures that can be taken in the mean time until customers are able to implement the software updates." RIM asks companies to make sure their BlackBerry Enterprise Server and BlackBerry Router are located behind the corporate firewall. RIM calls it an "internal−only vulnerability" that can be caused by an inside attacker.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=
HCQOZBHQGSYK0QSNDBCSKHSCJUMEKJVN?articleID=175800729

30. *January 03, Tech Web* — **Microsoft plans to patch zero−day Windows bug.** Microsoft plans to patch an increasingly−dangerous zero−day vulnerability in Windows next week as part of its monthly security update, the Redmond, WA,−based developer said Tuesday, January 3. "Microsoft has completed development of the security update for the vulnerability," a company spokesperson stated. "The security update is now being localized and tested to ensure quality and application compatibility." The move is just the latest in the week−long story of a new vulnerability uncovered in Windows' rendering of WMF (Windows Metafile) images, and an increasingly long list of both exploits and Websites using these exploits to hack into PCs. As far as some researchers are concerned, Microsoft's promise is overdue.
Source: http://www.securitypipeline.com/news/175800841;jsessionid=HC
QOZBHQGSYK0QSNDBCSKHSCJUMEKJVN

31. *January 02, SecuriTeam* — **Nortel SSL VPN cross−site scripting and command execution.** The Nortel SSL VPN is a remote access security solution. By using secure sockets layer (SSL) as the underlying security protocol, Nortel SSL VPN allows for using the Internet for remote connectivity and the ubiquitous Web browser as the primary client interface. Due to insufficient input validation within the Web interface of Nortel's SSL VPN appliance, it is possible to hide commands in links to certain pages of the Web interface. As the Java Applet which is called from those Web pages is cryptographically signed, it may execute operating system commands with the privileges of the user sitting in front of the browser. An attacker can thus supply a victim with malicious link where remote commands are hidden. If the victim clicks on the link

and logs onto the SSL VPN Web interface (where it is automatically taken), arbitrary commands are executed locally on the client of the victim.
Source: http://www.securiteam.com/windowsntfocus/5GP060KHFE.html

Internet Alert Dashboard

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 Website.
*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:
US−CERT 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

Additional details and workarounds are available in VU#181038:
http://www.kb.cert.org/vuls/id/181038

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

For further details please see:
http://www.kb.cert.org/vuls/id/829400
http://www.kb.cert.org/vuls/id/392920
http://www.kb.cert.org/vuls/id/570768

SANS: MSI installer file for WMF flaw available (NEW): SANS reports that they now have a .msi installer file available for version 1.4 of Ilfak Guilfanov's unofficial patch for the Windows .WMF flaw.

Details available at: http://isc.sans.org/diary.php?storyid=1010

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6346 (gnutella−svc), 25 (smtp), 445 (microsoft−ds), 27015 (halflife), 139 (netbios−ssn), 80 (www), 135 (epmap), 6881 (bittorrent), 4672 (eMule) 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

Nothing to report.

[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

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.