Department of Homeland Security Daily Open Source Infrastructure Report for 09 January 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

Daily Highlights

- The Department of Homeland Security has announced the expansion of Operation Stonegarden, an initiative that will give states additional funding and flexibility to strengthen America's borders. (See item 13)
- The Department of Homeland Security has announced the creation of new Border Enforcement and Security Task Forces, as part of the Department's Secure Border Initiative aimed at increasing control over America's borders. (See item 14)
- The Associated Press reports officials in and around Washington, DC, are considering new approaches to disaster response, such as improve traffic signals and signs, and find ways to restrict access to major evacuation routes. (See item 27)

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 06, New York Times* — **Upgrading of Indian Point's sirens ordered.** On Thursday, January 5, the United States Nuclear Regulatory Commission issued a preliminary order yesterday requiring the owner of the Indian Point nuclear power plant to install a backup power source for its warning sirens by early next year. A final order could be issued by the end of the

month if the owner, Entergy Nuclear Northeast, waives a hearing. The company would then have until Monday, January 30, 2007, to make the changes so that the sirens could continue to function during a power failure. Last year, Congress passed legislation that had the effect of requiring the Indian Point plant, which is 35 miles north of Midtown Manhattan in Buchanan, N.Y., to have backup power for its emergency notification system. Entergy officials said that the installation of generators at each of the 156 sirens was impractical, given the risks of vandalism and theft. The company decided on stationary four−way speakers, which could be powered by smaller backup batteries.
Source: http://www.nytimes.com/2006/01/06/nyregion/06siren.html?oref =login

2. *January 05, Agence France−Presse* — **France to develop fourth−generation nuclear reactor.** French President Jacques Chirac announced plans to build a prototype fourth−generation nuclear reactor by 2020 as well as symbolic targets for cutting France's reliance on oil in the coming decades. Chirac said that France, which is the world's second producer of atomic energy after the United States, needed to "stay ahead in nuclear energy". Addressing business leaders and unions, Chirac said he had "decided to immediately launch work by the French Atomic Energy Commission (CEA) on a prototype fourth−generation reactor, to go into service in 2020". Chirac also said that oil would be gradually phased out in favor of alternative fuels on the country's public transport networks. National rail operator SNCF and the Paris metro company RATP "should not consume a drop of oil in 20 years' time," he said. Chirac's speech came hard on the heels of a gas dispute between Russia and Ukraine, which briefly disrupted provision to Europe and left many countries questioning their reliance on Russian energy supplies. Most reactors currently in service in the world are generally referred to as second−generation reactors. The third−generation European Pressurized Water Reactor (EPR) is to replace the 58 reactors of France's 19 atomic power plants, starting in 2012.
Source: http://news.yahoo.com/s/afp/20060105/wl_afp/francepoliticsec onomy_060105181742

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *January 04, Manufacturing and Technology News* — **Department of Defense is vulnerable to loss of circuit board industry.** The rapid decline of the U.S. printed circuit board industry should be raising red flags and a plan of action at the Pentagon, according to a new report from the National Research Council (NRC). With U.S. production projected to fall below 10 percent of world output (down from 42 percent in the mid 1980s), the military could soon be facing a crisis in finding U.S. companies capable of producing highly sophisticated circuit boards and assemblies for weapons systems needed to field a "netcentric" military force, says the report entitled "Manufacturing Trends in Electronics Interconnect Technology." The diminution of the printed circuit board (PCB) industry raises fundamental questions as to how the Department of

Defense (DoD) is going to handle technology development and assurance of supply in a global economy. The NRC committee spent a year assessing the state of the printed circuit board industry and its impact on DoD. It recommends that DoD affirm its "critical" dependence on the industry; that it start an assessment of its economic health by collecting data; and that it increase support for the few national PCB research facilities that do exist.
Manufacturing Trends in Electronics Interconnection Technology report summary:
http://www.nap.edu/reportbrief/11515/11515rb.pdf
The full report is available online: http://www.nap.edu/books/0309100348/html/
Source: http://www.manufacturingnews.com/news/06/0104/art1.html

[Return to top]

Banking and Finance Sector

4. *January 06, The Register (UK)* — **Data sharing tops UK banks' anti−fraud agenda.** Data sharing and coordination top the agenda of UK banks in the fight against financial fraud, according to an exit poll at a recent financial crime conference. The survey −− conducted by data integrity firm Datanomic after a conference organized by the British Bankers Association −− found data sharing was a key concern for banks this year, with 40 percent of delegates listing it as a top concern. The need for better data sharing came out ahead of ID fraud (30 percent) and managing risk (15 percent). Fraud prevention and detection were the top concern for only five percent of delegates polled. Three−quarters of bankers said that recent terrorist actions had made thorough matching of customer data against sanctions lists more important to their business. Despite this, 40 percent admitted that they do not have an automated solution in place for sanctions matching.
Source: http://www.theregister.co.uk/2006/01/06/uk_bank_fraud_survey /

5. *January 06, Chicago Tribune (IL)* — **Illinois governor fights cell records theft.** In an attempt to protect residents from identity theft, Illinois Governor Rod Blagojevich announced a series of proposals to crack down on the unauthorized release of private information by brokers and phone companies. The legislation would make Illinois the first state to fight "pretexting," which is the practice of pretending to be the account holder or have authorized use of an account, according to a release from the governor's office. The proposed legislation would prevent the unauthorized access to cell phone call records, long distance call records, and other personal records. The laws would also require phone companies to maintain appropriate privacy measures and inform consumers of a security breach. Brokers and phone companies would be breaking the law if private information, such as identifying information or the location of any Illinois resident or business, was released or sold. There would also be increased criminal penalties for hacking phone record information and employee theft of phone company information. According to the Electronic Privacy Information Center, there are at least 40 Websites practicing cell phone "pretexting," and in most cases the brokers only need a billing address and another piece of personal information to obtain the records.
Source: http://www.chicagotribune.com/news/local/chi−060106cellphones,1,1251004.story?ctrack=1&cset=true

6. *January 06, Reuters* — **Police apprehend major Columbian drug and money laundering ring in Britain.** Britain said on Friday. January 6, it had jailed 34 people involved with a

mainly Colombian gang who ran the biggest cocaine and money−laundering operation ever to be uncovered in the country. The network was so substantial that the gang supplied drugs to every major UK city, and after their arrest the price of cocaine on Britain's street rose by 50 percent. Police said up to 20,000 people worldwide were believed to have been involved in the money−laundering operation. "We believe we have ripped the heart out of drug trafficking into the UK," said Detective Superintendent Martin Molloy from the National Crime Squad (NCS). In total the gang −− 25 from Colombia, four from Spain, three from England, and one each from Canada and Panama −− received prison terms totaling more than 300 years. Detective Sergeant Ian Floyd said it was also one of the first times suspected drug barons at the head of a network in Britain had been caught. "They were very important. They were probably the primary drugs and money−laundering group within the UK," he told Reuters.
Source: http://news.yahoo.com/s/nm/20060106/wl_canada_nm/canada_crime_britain_colombians_col_1

7. *January 05, Air Force Times* — **'Phishing' warning issued to users of Air Force Website.** Airmen are being warned to watch for a bogus e−mail message that's designed to look like an official Air Force message, an apparent scam to steal airmen's identity information. Users of the Air Force Portal Website −− https://www.my.af.mil −− have been warned to be wary of e−mails asking them to update their Air Force Portal account information. 1st Lt. Stephen Fox, a spokesperson for the Electronic Systems Center at Hanscom Air Force Base, MA, which oversees the Air Force Portal, said that because the scam is under investigation, officials wouldn't discuss the fraud, including how many airmen may have been victimized or whether the scam had resulted in a breach of the Website's security. When airmen click onto links in the bogus e−mail, they are connected to a site designed on quick glance to look like the Air Force Portal, the warning said. The real portal site shows the Web address −− https://www.my.af.mil −− at the top of the Internet browser. The Air Force Portal allows airmen anywhere to reach hundreds of Air Force Web pages, databases, and other programs. All airmen are expected to register with the portal.
Source: http://www.airforcetimes.com/story.php?f=1−292925−1449582.ph p

8. *January 05, FinanceTech* — **Hackers target financial services.** The financial services industry is the number one target of security probes by criminal hackers, according to a report by network security provider Counterpane Internet Services. The most predominant attacks are TCP probes looking for printers, probes looking for the UNIX Finger application and probes looking for IMAP 4 (Internet Message Access Protocol) services. The financial services industry was the target of 50 percent of all security probes that occurred on Counterpane's more than 500 monitored networks worldwide, the company reports. While probing is common and typically is attended to on a weekly basis, 333 instances of probes across all industries were significant enough to require Counterpane to notify its customers immediately. Further, financial services ranks second in total security events, accounting for 18 percent of those that occurred in 2005, Counterpane says. (The technology sector ranked first, with 26 percent.) The security provider also points out that many of the occurrences of network probing originated in Romania −− a known location of organized crime and criminal hacking.
Report (requires registration): http://www.counterpane.com/pr−20051115.html
Source: http://www.financetech.com/news/showArticle.jhtml?articleID= 175801626

[Return to top]

Transportation and Border Security Sector

9. *January 08, Associated Press* — **More than half South Carolina rails lack electronic warning system.** More than half the railroad tracks in South Carolina do not have an electronic system to warn oncoming trains that there is danger ahead. An analysis by The (Columbia) State newspaper showed that 1,100 miles of the state's 2,000 miles of track are in so called "dark territory." George Gavalla, who works for a private railroad consulting firm, said the Federal Railroad Administration could mandate the warning systems for some sections of track depending on traffic, type of material being transported, and number of people living nearby. There are about 100 South Carolina towns with populations of less than 15,000 along the track with no signals. The tracks are owned by CSX and Norfolk Southern. The National Transportation Safety Board has recommended that railroads install warning devices, such as a strobe light, at manual switches to alert crews to problems. But those aren't considered full−fledged warning systems because they cannot detect other rail problems, such as a broken rail. Only the Federal Railroad Administration can order the companies to install the devices and that agency has no plans to do that.
   Source: http://www.thestate.com/mld/thestate/news/local/13579795.htm

10. *January 06, Associated Press* — **Woman dies on America West flight from Cleveland to Phoenix.** A 45−year−old woman died on an America West flight from Cleveland to Phoenix, forcing an unscheduled landing in Colorado Springs on Thursday, January 5. The passenger was found unconscious in her seat on America West Flight 29. A cardiologist and an EMT on board performed CPR for 30 minutes before the plane landed at 1:10 p.m. MST. Police said other passengers reported seeing the woman take prescription medication shortly before she passed out.
   Source: http://www.usatoday.com/travel/news/2006−01−06−flier−death_x .htm

11. *January 06, Associated Press* — **Alaska Airlines jet damaged in on−ground incident.** An Alaska Airlines Boeing 737−700 jet was damaged at Seattle−Tacoma International Airport (Sea−Tac) after being inadvertently shoved into a jetway by a vehicle used to load baggage. No one was injured. The jet was moved about three feet on Thursday, January 5, by a push tug, causing the right engine to hit a baggage loader and the entry door on the left side of the plane to collide with the jetway at Gate D2, Alaska Airlines spokesperson Amanda Tobin said. Damage to the aircraft was minor and the plane's engines were not on at the time, Tobin said. The push tug was being operated by an employee of Menzies Aviation, who immediately alerted Alaska Airlines. Alaska Airlines informed the Federal Aviation Administration and the Port of Seattle. The airline was investigating and the worker involved was suspended, Tobin said. Alaska Airlines hired Britain−based Menzies to provide baggage handling and other ramp services after laying off nearly 500 ramp workers at Sea−Tac in May. In a statement then, Alaska said hiring Menzies would save $13 million a year.
   Source: http://www.usatoday.com/travel/news/2006−01−06−alaska−damage_x.htm

12. *January 06, Boston Globe* — **Night closings of the Big Dig's tunnels to end.** Major leak repairs and sealing of Boston’s Big Dig tunnels will be done by the end of next week, promising an end of nearly three years of late−night tie−ups and spaghetti−like detours, officials said on Thursday, January 5. By the end of the month, officials plan to open the

Interstate 93 tunnels around the clock for the first time. The completion of the work marks another milestone for the $14.6 billion project, which was scheduled to be substantially complete in September. Since shortly after the northbound tunnel opened in March 2003, crews repairing leaks and doing other tunnel construction have had to block overnight traffic on most weeknights. The overnight work picked up after a massive September 2004 rupture closed portions of the northbound tunnel and led to disclosure of hundreds of leaks. The Big Dig, which is to carry 245,000 vehicles a day by 2010, was the first major road project in the country to use slurry walls as the tunnel's only walls. After the September 2004 leak, officials found that some of the slurry walls were poured incorrectly and had allowed dirt and other debris to get into the concrete. Underground water then seeped through that dirt and penetrated or created soft spots in the tunnel walls.
Source: http://www.boston.com/news/traffic/bigdig/articles/2006/01/06/night_closings_of_the_big_digs_tunnels_to_end/

13. *January 06, Department of Homeland Security* — **DHS expands Operation Stonegarden to bolster border security efforts.** The Department of Homeland Security (DHS) has announced the expansion of Operation Stonegarden, an initiative that will give states additional funding and flexibility to strengthen America's borders. The new grant guidance reflects Secretary Michael Chertoff's top priorities to strengthen border security and establish a common approach to enhancing preparedness capabilities throughout our nation. As part of the 2006 fiscal year Homeland Security Grant Program, the Law Enforcement Terrorism Prevention Program (LETPP) will award $400 million in grants to states based on risk and need. In fiscal year 2006, the LETPP allows for up to 25 percent of the funds awarded to each border state to be used for border protection. Under the auspices of the LETPP, DHS plans to reinitiate the highly successful Operation Stonegarden as a means of improving border security and countering the terrorist threat. During fiscal year 2005, Operation Stonegarden was extremely effective in bolstering border security in areas deemed vulnerable or at risk with 214 state, local, and tribal agencies working a total of 36,755 man−days along the Mexican and Canadian borders. Funding will be contingent upon recipients having an approved operational plan developed jointly between state, tribal and local law enforcement officials and U.S. Customs and Border Protection.
Source: http://www.dhs.gov/dhspublic/display?content=5332

14. *January 06, Department of Homeland Security* — **DHS announces task forces to combat crime at the Southwest border.** The Department of Homeland Security (DHS) Secretary Michael Chertoff announced on Friday, January 6, the creation of new Border Enforcement and Security Task Forces, as part of the Department's Secure Border Initiative aimed at increasing control over our borders. These task forces will be nationally integrated teams with federal, state, and local representation specifically directed at cross−border criminal activity. "These new task forces will take a comprehensive approach to dismantling criminal organizations that exploit our border," said Secretary Chertoff. Border Enforcement and Security Task Forces will focus on every element of the enforcement process, from interdiction to prosecution and removal, with the goal of eliminating the top leadership and supporting infrastructure that sustains these cross−border organizations. They will leverage federal, state, tribal, local, and intelligence entities to focus resources on identifying and combating emerging or existing threats. The next Border Enforcement and Security Task Force will be established in Arizona, after DHS conducts a threat assessment of that area. DHS will conduct similar assessments as it

establishes additional task forces and will constantly measure results in order to refine and focus enforcement actions.
Source: http://www.dhs.gov/dhspublic/display?content=5331

[Return to top]

Postal and Shipping Sector

15. *January 06, Federal Times* — **CFO says 2006 will be challenging for Postal Service.** Though encouraged by a fiscal year−end balance sheet that was happier than anything seen for decades, the U.S. Postal Service is nonetheless gearing up for a challenging 2006 that will likely see the agency finish $2 billion in the red. This would follow two years running of net surpluses, the first since the agency was reorganized in 1971. The deficit will result in good part because of expected increases in costs, almost across the board. Last year costs for such things as fuel, retirement benefits, cost−of−living adjustments and health benefits rose an average five percent, a rate well above inflation and enough to add more than $3 billion to overall costs. Most of those costs will increase substantially again in 2006, according to Postal Service Chief Financial Officer (CFO) Richard Strasser. One of the biggest financial burdens for the Postal Service is health care for workers and retirees, which cost $6.5 billion in 2005 and will cost about $7 billion in 2006, Strasser said. With the anticipated higher costs, the Postal Service says it will look to cut infrastructure further, continue to add technology to increase productivity, and work to increase mail volume, especially in the promising business mail categories.
Source: http://federaltimes.com/index2.php?S=1439811

16. *January 06, Associated Press* — **U.S. postage rates increased on Sunday.** It will cost Americans two cents more to mail a letter starting Sunday, January 8. First−class postage rises to 39 cents for the first ounce. The increase follows legislation requiring the Postal Service to place $3 billion in an escrow account this year. Another rate boost is likely next year to cover rising costs for the agency. Stamp prices last went up in June 2002. Many rates, such as parcel post and advertising mail, vary by distance or whether the material is presorted. Increases in certified mail, deliver confirmation for priority and first class parcels, return receipt, both original signature and electronic, and money orders also will begin January 8.
Source: http://sfgate.com/cgi−bin/article.cgi?f=/n/a/2006/01/07/fina ncial/f024733S72.DTL

[Return to top]

Agriculture Sector

17. *January 07, Associated Press* — **Wild hogs frustrate Georgia farmers.** Farmers across Georgia are struggling to deal with wild hogs that eat up their crops and spread disease. From Texas to Florida, the feral pigs are eating anything they can find, from turtle eggs to garbage to the carcasses of other animals. And their numbers are growing. Steve Ditchkoff, an associate professor of wildlife at Auburn University, calls wild hogs "one of the greatest ecological threats to the U.S., and right now, we have no way to control them." Ditchkoff is organizing the 2006 National Conference on Wild Pigs, to be held in Mobile, AL, this May. About 200 wildlife biologists and others are expected to come from across the country to talk about the

spread of wild hogs. In Georgia, the hog population is concentrated on the coast and along the streams and swamps of south and central Georgia. Farmers also worry about the wild hogs spreading diseases to their domestic animals. Both pseudorabies and swine brucellosis have been found in Georgia hogs.
Source: http://www.macon.com/mld/macon/13573129.htm

18. *January 07, Associated Press* — **Wyoming gets brucellosis−free plan.** Wyoming has until early February to respond to federal recommendations on how the state can regain its brucellosis−free status for livestock. The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) put together a Wyoming Brucellosis Review Team −− a group of experts who determined what steps the state must take to regain its disease−free status. The state had applied to regain its disease−free status in early December. The review team recommends that Wyoming take the following measures: require registration of cattle dealers and require record−keeping by dealers of each transaction; require adequate surveillance and vaccination to mitigate the risk of reinfection in places where livestock are at risk of exposure to infected wildlife; identify the measures the state will take to prevent re−infection of livestock from wildlife in a formal memorandum of agreement between the state and APHIS; and streamline reporting and tracking of brucellosis test results into federal database systems.
Source: http://www.billingsgazette.com/index.php?id=1&display=rednews/2006/01/07/build/wyoming/60−brucellosis−plan.inc

19. *January 06, RFID Journal* — **Colorado looks to active RFID for cervids.** After completing a trial of passive low frequency and UHF RFID (radio frequency identification) tags for cervid tracking, the Colorado Department of Agriculture has determined that active RFID tags may be the only way to gain the 100 percent read rate it seeks for cervid herds in the state. Colorado mandates that ranchers test dead elk and fallow deer for chronic wasting disease (CWD). If an animal decomposes before being tested, neither ranchers nor the state can determine if it died of the lethal and contagious disease. In the most recent of two Colorado cervid pilots—using passive UHF RFID tags and interrogators (readers) the state's agriculture department was able to read 100 percent of the tags on one of the three herds tested, but considerably less on the other two, says Scott Leach, the department's CWD field investigator. Leach says he has not yet tried to use a passive RFID system to track an animal, live or dead. He adds, however, that active RFID equipment manufacturers have indicated tracking of animals may be possible. In the meantime, passive RFID systems allow the ranchers to recognize the loss of an animal and search for it.
Source: http://www.rfidjournal.com/article/articleview/2073/1/1/

[Return to top]

Food Sector

20. *January 05, Farm & Ranch Guide* — **Elevators could be among first inspected when Food and Drug Administration starts enforcing bioterror law.** Bulk grain elevators could be the first places to be inspected by the Food and Drug Administration (FDA) under its bioterror law. In June, the FDA will start enforcing the new bioterror law related to recordkeeping of food products. Under the law, records for feed will need to be kept one year. At a recent Integrated Crop Management Conference, Charles Hurburgh, an Iowa State University professor of

agriculture, said while listening to an FDA presentation, bulk grain elevators are on the FDA's radar. He expects elevators to be among the first inspected because the FDA knows food processors and food companies can follow the paper trail. Under the FDA inspections or audits, they will likely look at ways to trace grain to where they got it. In the meantime, there are procedures for grain elevators to prepare for enforcement of the law. Some suggestions include: Put the initial bin assignment on scale tickets, date and time stamp scale tickets, record date and time of in−house transfers, and record load−out information, such as time to fill and percent gate openings. In addition, Hurburgh suggests elevators develop a flow chart and written procedures of their operations.
Source: http://www.farmandranchguide.com/articles/2006/01/05/ag_news/regional_news/news16.txt

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

21. *January 08, Sunday Times (United Kingdom)* — **Turkish deaths put Europe on bird flu alert.** The number of Turkish people thought to be infected with avian flu rose to more than 50 this weekend, prompting concern that the disease may be about to spread into Europe. Saturday, January 7, a British laboratory confirmed that a Turkish brother and sister who died last week had the H5N1 strain of avian flu. A third child from the same family in Dogubayazit, in eastern Turkey, has now died of avian flu and dozens more suspected cases have emerged. They are the first fatalities outside East Asia. Saturday, January 8, six more children who have tested positive for avian flu remained in a critical condition in the Turkish city of Van, near Dogubayazit. Another 24 suspected cases are being treated in a special ward in the university hospital. A further 18 patients with symptoms of the disease, most of them children, are being treated in hospitals in the eastern cities of Yozgat, Erzurum, and Diyarbakir. Other cases are being investigated. Mehdi Eker, the Turkish agriculture minister, confirmed that bird flu had also been identified in two dead ducks found by a reservoir near Ankara, the capital, about 750 miles west of Dogubayazit.
Source: http://www.timesonline.co.uk/article/0,,25149−1974978,00.htm l

22. *January 06, Agence France−Presse* — **Indonesian tests show man dies of bird flu.** Tests carried out by Indonesian authorities showed that a man who died this week had bird flu. Further tests will be carried out at a Hong Kong laboratory accredited by the World Health Organization to confirm the finding, said senior health ministry official Hariyadi Wibisono. "Local test results show that the man died of bird flu," he said Friday, January 6. Results are expected next week, he said. The man died Monday, January 2, after being treated for a day at Jakarta's Sulianti Saroso hospital, Indonesia's main bird flu treatment center. He was from Tangerang, a town southwest of Jakarta where there have been bird flu outbreaks.
Source: http://news.yahoo.com/s/afp/20060106/hl_afp/healthindonesiaf

lu_060106102208;_ylt=AoX6tw3dhNVRmxBJSj124V6JOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

23. *January 06, Associated Press* — **Many doctors in short supply of flu shots.** Many physicians complain much of this year's vaccine went to supermarket and discount chains instead of medical clinics. That's a problem for some people who are most at risk of life−threatening flu complications but aren't always healthy enough to wait in store lines. For thousands of Americans, especially those who are healthy, a flu clinic at the local drugstore or discount chain is easier and faster than making an appointment to see the doctor. However, doctors say chain stores don't necessarily give priority to the nearly 90 million Americans considered at high risk of flu complications. They also say it's often better for those patients to see their doctor, who can check their blood pressure, medications, and other concerns. A survey by the New Jersey Academy of Family Physicians found two−thirds who responded had received little or no vaccine by December, but 90 percent saw local stores giving shots. The U.S. Centers for Disease Control and Prevention (CDC) said about 88 million shots will have been distributed by the end of January. Medical groups and public health officials are so concerned about distribution problems they have made it a prime topic for their annual flu vaccine summit set for later this month.
CDC flu surveillance site: http://www.cdc.gov/flu/weekly/fluactivity.htm
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/06/AR2006010601254.html

24. *January 06, Reuters* — **Pandemic flu checklist for households issued.** There is no vaccine and drugs are in short supply but Americans may be able to ride out any bird flu pandemic if they stock up on supplies and keep their children clean, the U.S. government said on Friday, January 6. The U.S. Department of Health and Human Services' checklist illustrates just how little can be done to prevent widespread illness and disruption in the case of pandemic influenza. The checklist advises: teaching children to wash hands frequently and covering coughs and sneezes with tissues; having ready−to−eat canned meats, fruits, vegetables, soups, bottled water, and cleaning supplies on−hand for an extended stay at home; having any nonprescription drugs and other health supplies on hand; and talking with family members and loved ones about how they would be cared for if they got sick or what will be needed to care for them in another home.
Pandemic Flu Planning Checklist for Individuals and Families:
http://www.pandemicflu.gov/planguide/checklist.html
Source: http://news.yahoo.com/s/nm/20060106/hl_nm/birdflu_checklist_dc

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

25. *January 06, Federal Computer Week* — **Utah county makes records safer.** The Salt Lake County, UT, Recorder's Office has established a state−of−the−art disaster recovery program that will allow officials to securely access, via the Internet, 13 million public records stored in a redundant system at an offsite facility. The county's Recorder, Gary Ott, states although a natural disaster in Salt Lake County seems unlikely, the municipality lies along an earthquake fault. Ott, who has led the office for six years, said document preservation has been a high priority, and the office has made significant investments. The office stores deeds, titles and other property−related information, among other vital documents. The offsite or co−location site, which is geographically close enough to access but far enough away from the disaster zone, cost about $140,000 to establish, he said. The secure facility with redundant computer servers is privately owned and has 24−hour staff and generators to protect against power outages, hackers and other hazards. Ott said the office previously had tape backups of data. But if disaster had struck, it would have taken time to access the two terabytes of stored data. Now he can go online and operate as an office from anywhere.
Source: http://www.fcw.com/article91869−01−06−06−Web

26. *January 05, Global Security Newswire* — **House Democrat seeks new terrorist information−sharing unit.** In the latest of a series of proposals for easing exchanges of terrorism information among U.S. federal, state and local agencies, the top Democratic representative on antiterrorism matters is calling for a new office to facilitate "vertical" information−sharing. The new unit would convert classified intelligence into forms usable by state and local officials and would provide a channel by which terrorism information from state and local officials could reach federal authorities. House Homeland Security Committee's Bennie Thompson (D−MS) stated, "We must keep state, local and tribal law enforcement in the loop and engaged in law−enforcement intelligence…as it is now, they are not being given the information they need when they need it to identify potential terrorists or their methods." To jump−start progress, the Democrat called for creating a Vertical Intelligence Terrorism Analysis Link, modeled after the United Kingdom's Police International Counterterrorism Unit and Joint Terrorism Analysis Center. Those two units, according to the Democratic report, circumvent many obstacles to information sharing by allowing police and intelligence analysts to work side−by−side with a common mission.
Source: http://www.govexec.com/dailyfed/0106/010506gsn1.htm

27. *January 05, Associated Press* — **District of Columbia area officials consider evacuation and emergency plans.** Hurricanes Katrina and Rita, as well as the London subway and bus bombings, are prompting officials in and around the nation's capital to look at new approaches to disaster response. Maryland Transportation Secretary Robert L. Flannigan and others have noted that volunteers who responded to the Gulf Coast noted problems with housing displaced residents and supplying gasoline for evacuees and relief workers. Officials have worked to improve traffic signals and signs. More emergency vehicles are equipped with technology that changes signal lights, allowing them to reach incidents faster. In addition, officials from many jurisdictions have been studying ways to restrict access to major evacuation routes so those roads are not clogged by local traffic when they are needed. While Metro, the region's major mass transit system, does not have its own emergency corps, officials say their experience following the September 11, 2001, terrorist attack on the Pentagon indicates that its Metrorail and Metrobus operators could be counted on to transport passengers for as long as necessary.
Source: http://www.timesleader.com/mld/timesleader/news/breaking_new s/13558130.htm

[Return to top]

Information Technology and Telecommunications Sector

28. *January 05, CNN* — **Microsoft releases patch for WMF flaw.** Microsoft has released a patch for a vulnerability in some Windows graphics files. For more than a week, criminal hackers have been exploiting the flaw in Windows Meta File, or WMF. About 90 percent of computer users worldwide use some form of the Windows operating system. The company became aware of the malicious attacks Tuesday, December 27. What's especially dangerous about the attacks: Your computer could be infected with viruses, spyware or other malicious programs just by viewing a Webpage, an e−mail message, or an Instant Message that contains one of the contaminated images. Computer security experts have been dealing with scores of variations on the attack since it was discovered. "Nobody knew it was coming," security expert Rick Howard of Counterpane Internet Security said. "There was no security intervention or mitigation for it." Unlike infamous computer worms and viruses like Blaster, Code Red or I Love You, the WMF attack is not spreading like wildfire across the Internet. Most of the malicious efforts fit the patterns of recent attacks. They are not designed to earn bragging rights for a brash programmer, but instead are likely tied to theft, fraud and organized crime.
US−CERT Technical Cyber Security Alert TA06−005A: Update for Microsoft WMF vulnerability: http://www.uscert.gov/cas/techalerts/TA06−005A.html
Microsoft Security Bulletin MS06−001:
http://www.microsoft.com/technet/security/Bulletin/MS06−001. mspx
Source: http://www.cnn.com/2006/TECH/internet/01/05/wmfflaw/index.ht ml

29. *January 05, Associated Press* — **Iowa company wins $11 billion spam judgment.** A Clinton, IA−based Internet service provider was awarded an $11.2 billion judgment against a Florida man for sending millions of unsolicited e−mails advertising mortgage and debt consolidation services. The lawsuit, filed in 2003 by CIS Internet Services owner Robert Kramer III, also prompted earlier judgments against companies in Florida and Arizona worth more than one billion. The most recent judgment was issued Friday, December 23, against James McCalla of Florida, who is also barred from accessing the Internet for three years. The lawsuit claimed that McCalla sent more than 280 million illegal spam e−mails into CIS's network, which provides Internet connections in Eastern Iowa and parts of Illinois. Kramer's lawsuit initially named numerous defendants, many of whom were dropped from the lawsuit the last couple years. John Mozena, co−founder and vice president of Coalition Against Unsolicited Commercial E−mail (CAUCE), said Kramer's lawsuit will likely not solve the spamming problem. He said, "There have been regulatory actions and even criminal actions against spammers, but it has not made much of a dent in the total volume of spam we see...Spam is still roughly two−thirds of all e−mail on the Internet."
Source: http://www.press−citizen.com/apps/pbcs.dll/article?AID=/2006 0105/NEWS01/601050310/1079

30. *January 05, Space* — **Record set for space laser communication.** In a cosmic version of laser tag, NASA’s MESSENGER spacecraft and an Earth−based observatory successfully exchanged laser pulses with each other while millions of miles apart. The feat sets a new record for laser transmission in space, a process which may one day be used to communicate across

interplanetary distances and provide scientists with a powerful tool to measure the movement of planets and test fundamental principles in physics. MESSENGER was launched in 2004 on a six−year voyage to Mercury. In late May of 2005, scientists used the spacecraft's Mercury Laser Altimeter (MLA), an instrument designed to map Mercury's surface, to exchange laser pulses with NASA's Goddard Geophysical and Astronomical Observatory in Maryland. MESSENGER was approximately 15 million miles away at the time. The experiment, reported Thursday, January 5, marks the first successful back−and−forth exchange of laser signals between Earth and space. Two−way laser communication in space has long been a goal for NASA because it would enable data transmission rates that are 10 to 1,000 times higher than traditional radio waves. If the technical hurdles can be overcome, lasers would benefit not only communications, but basic science as well.
Source: http://www.space.com/missionlaunches/060104_laser_comm.html

31. *January 05, Chicago Sun−Times* — **Phone records are for sale via online data brokers.** The Chicago Police Department is warning officers their cell phone records are available to anyone −− for a price. Dozens of online services are selling lists of cell phone calls, raising security concerns among law enforcement and privacy experts. Criminals can use such records to expose a government informant who regularly calls a law enforcement official. Some online services might be skirting the law to obtain these phone lists, according to Sen. Charles Schumer (D−NY), who has called for legislation to criminalize phone record theft and use. In some cases, telephone company insiders secretly sell customers' phone−call lists to online brokers, despite strict telephone company rules against such deals, according to Schumer. And some online brokers have used deception to get the lists from the phone companies, he said. According to Schumer, a common method for obtaining cell phone records is "pretexting," involving a data broker pretending to be a phone's owner and duping the phone company into providing the information. "Pretexting for financial data is illegal, but it does not include phone records," Schumer said.
Source: http://www.suntimes.com/output/news/cst−nws−privacy05.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 which may be masquerading as a MS Word or MS Office document.
Opening a specially crafted WMF file which may be masquerading 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

More information about this vulnerability can be found in the following: US−CERT Vulnerability Note: VU#181038 − Microsoft Windows Metafile handler SETABORTPROC GDI Escape vulnerability http://www.kb.cert.org/vuls/id/181038

Technical Cyber Security Alert TA06−005A− Update for Microsoft Windows Metafile Vulnerability: http://www.us−cert.gov/cas/techalerts/TA06−005A.html
Cyber Security Alert SA06−005A − Microsoft Windows Metafile Vulnerability: http://www.us−cert.gov/cas/alerts/SA06−005A.html

US−CERT strongly encourages users and administrators to apply the appropriate updates as soon as possible. Microsoft has released an update to address this vulnerability in Microsoft Security Bulletin MS06−001: http://www.microsoft.com/technet/security/Bulletin/MS06−001. mspx

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 135 (epmap), 25 (smtp), 80 (www), 32801 (−−−), 6346 (gnutella−svc) 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