Department of Homeland Security Daily Open Source Infrastructure Report for 10 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 a Western Aircraft fuel truck struck an engine on a United Airlines jet waiting to leave a gate at the Boise, Idaho, airport causing damage that could cost millions to fix. (See item 9)

- The Chicago Tribune reports Chicago has launched an Internet−based emergency planning campaign that officials said is designed to stress personal preparedness thus making disaster readiness a part of every household. (See item 23)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

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 09, Bloomberg* — **Coal prices expected to drop in 2006, except in U.S.** The price of coal is expected to decline in much of the world this year from a record level because of increased exports from Indonesia, South Africa, and Australia. Analysts at National Australia Bank forecast a price decline of almost 20 percent, to less than $45 a metric ton. A shortage of digging equipment prevented production from meeting demand that rose in China, Europe, and the United States, where higher natural gas prices led some utilities to use more coal. While prices decline in Asia and Europe, U.S. coal costs will stay high, said James Rollyson, a coal industry analyst at Raymond James Financial in Houston. Utilities need to rebuild inventories,

and import terminals and railroads are operating at capacity, preventing a surplus outside the United States from entering the country, he said.
Source: http://www.iht.com/articles/2006/01/08/news/bxcom.php?rss

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

2. *January 09, InformationWeek* — **Instant Messaging buddy, or a hacker −− it's hard to tell.** Instant−messaging (IM) security vendors FaceTime Communications Inc. and IMlogic Inc. reported last week that malware delivered over instant−message clients has skyrocketed in recent months. FaceTime cites a more than 20−fold increase in the number of reported IM worm and virus variants since 2004. According to the Radicati Group, 85 percent of businesses of all sizes say instant messaging is taking place on their networks. IM attacks are getting more devious. FaceTime found one on AOL Instant Messenger and contacted AOL, as well as Microsoft and Yahoo, since many attacks are cross−platform. Virus attacks are getting more complex, too, moving away from simple social engineering. In late December, security vendors started seeing malicious code that went beyond a link or file and created automated responses to victim's queries. So a victim might ask his IM "buddy" if the file was safe, and the malicious bot would respond that it was. IMlogic discovered a bot that responded six different ways, depending on the question a victim asked.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=OJ2RW1LVCP1D2QSNDBOCKH0CJUMEKJVN?articleID=175802139

3. *January 08, Reuters* — **IDs of 50,000 Bahamas resort guests stolen.** The identities of more than 50,000 customers of major Bahamas resort Atlantis have been exposed to possible identity fraud following the theft of personal information from the hotel, the owners said. Kerzner International Ltd., owner of a 2,300−room Atlantis resort on Paradise Island, revealed details of the data theft in a document filed with the Bahamas Securities and Exchange Commission. Information stolen included names, addresses, credit card details, social security numbers, drivers license numbers, and bank account data, the filing said. The information appears to have gone missing from the hotel's computer database and was the work of either an insider or outside hacker. The Atlantis hotel management is notifying affected customers so they can take steps to protect themselves from possible identify fraud. The hotel is also providing, at no cost to customers, a credit monitoring service for a year. The filing by Kerzner said around 55,000 customers are thought to be affected. "To date, the resort has not received any evidence that the

information has been used to commit identity fraud or in any other manner adverse to its customers," the statement said. Atlantis has notified Bahamian and U.S. law enforcement agencies and is cooperating with them.
Source: http://news.yahoo.com/s/nm/20060108/wl_nm/leisure_kerzner_id entity_dc_1

4. *January 08, Oregonian* — **Banks locking in online security.** The number of Americans paying bills and monitoring account balances on the Internet has skyrocketed in recent years. About 40 million households −− accounting for almost one of every two U.S. bank and credit union accounts −− did at least some of their banking online last year, a figure that has nearly doubled since 2001. The nation's financial institutions have noticed, moving quickly to tailor their services and adjust their Websites to attract customers. However, spyware has increased too. Jim Bruene, editor of the Online Banking Report newsletter says, "[Spyware] was an activity that was unheard of just three years ago...It appeared in 2004 and grew exponentially in 2005." New anti−fraud rules that go into effect this year should make online banking safer, but they also will make it more complicated. Bruene expects the growth of Internet banking to slow this year as people react to the changes. Bank of America rolled out its new system in which users select a picture that will always appear when they log into the bank's site from their regular computer −− a security measure imposter sites would be unlikely to match. Bank executives say they are seeking to balance security against convenience.
Source: http://www.oregonlive.com/news/oregonian/index.ssf?/base/business/1136613360304540.xml&coll=7

5. *January 07, SecureIDNews* — **Experts weigh in on bank responses to Federal Financial Institutions Council guidelines.** Many banks and credit unions are charging full speed ahead to improve the security of online banking. The recent guidelines put out by the Federal Financial Institutions Council (FFIEC) instruct banks to analyze risks of fraud attacks and enhance systems with some form of two−factor authentication. "The FFIEC guidance has had a huge impact of making people move," says Stu Vaeth, chief security officer at Diversinet, a company that develops soft tokens and provisioning for two−factor authentication. "It's putting a lot of the banks over the edge, saying, let's do something now." Banks also want to do something because of the growing media attention to phishing, identity theft, and online banking risks. Because of the lack of a single, authentication standard for all online transactions, you have to use multiple hard tokens for different transactions...This is perhaps one the biggest reasons why the sale of OTP [one−time password] devices hasn't exploded in America, says Vaeth. Although the larger 180 or so national institutions have been aware of the need to build to build stronger online security systems to deter fraud, smaller institutions are still trying to figure out the best solution, says George Tubin, a security analyst with TowerGroup.
Source: http://www.secureidnews.com/library/2006/01/07/experts−weigh−in−on−bank−responses−to−ffiec−guidelines/

6. *January 06, CNNMoney.com* — **Thieves net $100,000 in Washington Mutual ATM scheme.** A sophisticated group of thieves used technical trickery to steal ATM card information −− and over $100,000 −− from customers at two New York City Washington Mutual branches. The thieves rigged fake keypads and bank−card slots onto ATMs to gather card information and encoded the information on new cards, police say. They then used the new, fraudulent cards for withdrawals from approximately 50 Washington Mutual accounts at other ATM locations. The

two Washington Mutual branches were on Canal Street in lower Manhattan and on Hylan Boulevard on Staten Island. Images of the suspects were recorded on the bank's security cameras. John Hall of the American Bankers Association said, "This is a very unusual crime because of the sophistication it requires...The ATM system is hard to compromise because it requires two separate keys −− the card and the PIN −− and PINs are especially hard to get." Hall said that ATM fraud was more common at non−bank ATMs, where the security is less sophisticated. The Electronic Funds Transfer Association, an industry trade group, has worked to secure ATM transactions for years, including requiring extensive background checks for non−bank ATM operators. The suspects remain at large.
Source: http://money.cnn.com/2006/01/06/news/atm_fraud/index.htm

7. *January 06, Computer Weekly* — **General Electric cleared to transfer employee data overseas.** The UK's Information Commissioner has made use of new procedures governing the transfer of personal data outside the European Economic Area, by authorizing General Electric to pass employee information to parts of the group situated overseas. The move is said to be the first time that the data protection watchdog has authorized the transfer of employee data on the basis of what are known as "binding corporate rules." European firms are largely restricted by the terms of the Data Protection Directive of 1995 as to what data can be transferred or stored in countries without equivalent rules and enforcement procedures. Such transfers are forbidden unless the country or territory to which the transfer will be made can show an adequate level of protection for the rights and freedoms of data subjects. Only then will the transfer be authorized by the appropriate supervisory authority. But the procedures used in obtaining authorization are complex and have made it difficult for multinational corporations to function efficiently. Until now, authorizations have only been granted if a so−called Safe Harbour agreement exists with the recipient country, the transfer is within one of the allowed exceptions, or there is a contract.
Source: http://www.computerweekly.com/Articles/2006/01/06/213554/GeneralElectricclearedtotransferemployeedataoverseas.htm

8. *January 06, Network World* — **Three more states add laws on data breaches.** Companies struggling to keep up with a patchwork of U.S. state laws related to data privacy and information security have three more to contend with, as new security−breach notification laws went into effect in Illinois, Louisiana and New Jersey on Sunday, January 1. New Jersey's Identity Theft Prevention Act requires businesses to destroy all unneeded customer data and to notify consumers when sensitive data about them has been accessed by an unauthorized person. Louisiana's Database Security Breach Notification Law requires entities that collect information on the state's residents to notify affected individuals of security breaches involving their confidential data. Government officials also need to be notified, according to the law. Illinois' Personal Information Protection Act is similar, although it doesn't require companies to inform the state government when breaches occur. For companies that do business nationally or in various states, the smorgasbord of state laws poses a growing problem, because the measures often specify different triggers for notifications and set varying requirements on what needs to be disclosed, to whom and when, said Kirk Herath, chief privacy officer at Nationwide Mutual Insurance Co. in Columbus, OH.
Source: http://www.networkworld.com/news/2006/010606−data−breaches−law.html?fsrc=rss−security

[Return to top]

Transportation and Border Security Sector

9. *January 09, Associated Press* — **Fuel truck hits United Airlines jet at Boise airport.** A fuel truck struck an engine on a United Airlines jet waiting to leave a gate at the Boise, ID, airport, causing damage that could cost millions to fix, officials said. No one was injured. The Western Aircraft fuel truck failed to stop while approaching the Boeing 737 Sunday afternoon, January 8, and both the engine and the truck were damaged, airport police Sgt. Bruce Gard said. The plane was grounded and more than 100 passengers on United Flight 352 to Denver had to be put on other flights, with some forced to wait overnight, airline spokesperson Robin Urbanski said. A mechanical failure appears to be the reason for the collision, Gard said. The truck driver was ordered to undergo a blood test, although there was no indication that he was intoxicated, he added.
   Source: http://www.usatoday.com/travel/news/2006−01−09−united−fueltr uck_x.htm

10. *January 09, Associated Press* — **Airline to use runway crash−avoidance gear.** Deutsche Lufthansa AG Airlines will install a runway collision−avoidance system developed by Honeywell International Inc. on its fleet of about 250 planes, Honeywell said Friday. The safety equipment, called the Runway Awareness and Advisory System, should begin during the second quarter of this year. The system is designed to prevent runway incursions and accidents by alerting cockpit crews about runway distances, the presence of other aircraft or other potential problems. The system "will provide us with an extra margin of safety during ground operations," Claus Richter, vice president for operational support and deputy chief pilot for Lufthansa, said in a statement. Germany's Lufthansa becomes the seventh airline to buy the system, after companies including Air France−KLM, United Airlines, Alaska Airlines, and FedEx. The system works by using global positioning technology to compare the aircraft's location with a database of airport runways to determine the plane's exact location on the airfield. The system can alert pilots when they enter a runway and provide audio alerts in situations such as landing or takeoff on a short runway, an inadvertent attempt to take off from a taxiway or an aborted takeoff or long landing, when it can call out remaining runway distance.
    Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/06/AR2006010601459.html

11. *January 09, Transportation Security Administration* — **Two Washington area airports have explosives detection machines.** The Transportation Security Administration (TSA) on Monday, January 9, announced that it has deployed explosives detection trace portal machines to Ronald Reagan Washington National Airport (DCA) and Washington Dulles International Airport. The two airports join Baltimore−Washington International and 23 others nationwide in a program designed to prevent explosives material from getting on−board commercial aircraft. “The trace portal is a sophisticated tool that allows us to detect a broad range of explosive materials quickly and efficiently,” said Pat Hynes TSA’s Federal Security Director at DCA. Passengers identified as needing additional screening, as well as passengers selected at random, will pass through the trace portal for explosives detection screening. As passengers enter the trace portal, they are asked to stand still for a few seconds while several “bursts” of air are released, dislodging microscopic particles from passengers that are then collected and analyzed for traces of explosives. A computerized voice indicates when a passenger may exit the portal.

TSA officers will take necessary and appropriate steps to resolve alarms. TSA will continue to increase its explosives detection capabilities and expects to announce the next round of airports to receive these trace portal machines in the coming weeks.
TSA Website: http://www.tsa.gov
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 019b3f9

[Return to top]

Postal and Shipping Sector

12. *January 06, Federal Computer Week* — **Final rule defines postal service.** The Postal Rate Commission has issued a final rule on January 4, defining the term postal service, ending a lengthy public rule−making process. The commission’s next step will be to decide which of the new electronic services that the U.S. Postal Service (USPS) now offers fit that definition. The commission has authority to regulate the price USPS charges for any new postal service. In the text of the final rule, the commission states USPS officials are unhappy with the commission for defining postal service broadly enough to encompass any number of electronic services that USPS might offer in the future. USPS maintains that the commission has overstepped its jurisdictional authority. Under a definition of postal service that includes electronic services, the commission says it has the authority to approve or disallow such services and to regulate what USPS charges for them. The commission set a February 16 deadline for USPS to update the group's members on the status of 14 electronic service offerings that were the subject of a Consumer Action group complaint that led to the recent rulemaking. The new rule takes effect 30 days after its publication in the Federal Register.
Source: http://www.fcw.com/article91885−01−06−06−Web

[Return to top]

Agriculture Sector

13. *January 09, Associated Press* — **Citrus canker law under review.** A state law requiring the removal of trees within 1,900 feet of one infected with citrus canker is being reviewed by the Florida Department of Agriculture in the aftermath of four damaging summer hurricanes. The storms that struck Florida last year caused an estimated $2.2 billion in damage to the state’s crops and farming infrastructure and are also thought to have spread the diseases that threaten the state’s nine billion dollar citrus industry. Agriculture officials estimated Wilma and Katrina could be responsible for spreading canker to 183,000 acres, or a quarter of the state’s commercial citrus groves. Once canker is found in a grove, the state requires that citrus trees within a 1,900−foot radius be destroyed. Any change would have to be done by the Legislature. After a decade−long battle, state and federal agriculture workers had been close to eliminating citrus canker, which causes fruit and leaves to drop prematurely, but hurricanes the past two summers have spread the disease to new areas in the heart of the state’s citrus production. Citrus canker is caused by bacteria that causes blemishes on fruit, making it harder to sell.
Source: http://www.news−press.com/apps/pbcs.dll/article?AID=/2006010 9/NEWS0105/60108002/1075

14. *January 08, Observer−Dispatch (NY)* — **Researchers to study deer herds.** Researchers from the State University of New York College of Environmental Science and Forestry will be tracking scores of Central New York deer by satellite for a year in an effort to learn more about their habits and the potential spread of chronic wasting disease (CWD). Deer will be trapped and fitted with collars holding global positioning systems (GPS) that will allow their locations to be marked every five hours for one year. In addition to GPS units, the collars will have VHF capability that enables tracking through radio telemetry. The deer will be monitored weekly to make sure they are healthy and that the collars are working properly. The location of each deer at each point in time will be recorded on a chip, which will have a record that includes the animal's longitude and latitude, the altitude and air temperature, the time and date. The goal is to use the information to make a computerized model predicting how disease is likely to spread through a population of animals and across geographic features. The researchers will be able to build computer models of the deer's seasonal movements and the way their movements react to features on the land, both natural and manmade.
Source: http://www.uticaod.com/apps/pbcs.dll/article?AID=/20060108/SPORTS/601080327/1030

[Return to top]

Food Sector

15. *January 09, Associated Press* — **South Korea, U.S. open talks on beef imports.** South Korea and the U.S. began talks Monday, January 9, on lifting South Korea's two−year−old ban on imports of American beef. The two−day meeting in Seoul was not expected to lead to an immediate reopening of what was previously the third−largest market for U.S. beef after Japan and Mexico. One issue expected to dominate the discussions was whether South Korea should resume imports of beef ribs, which accounted for more than 60 percent of American beef shipments before the ban. South Korea says for now it will only consider importing boneless meat, citing concerns some material inside bones could be dangerous to consume. South Korean shut its doors to U.S. beef imports in December 2003 after the first U.S. case of mad cow disease. 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.cbsnews.com/stories/2006/01/09/ap/tech/mainD8F11G 000.shtml

16. *January 09, Tampa Bay Business Journal (FL)* — **Food label changes now in effect.** Companies looking to sell food across the country have some new guidelines in 2006 that are expected to help consumers stay away from food allergies and artery−clogging ingredients. Food manufacturers now are required to list "straightforward" language for any of the eight major food allergens that might be found in their products. This includes peanuts, nuts, fish, shellfish, eggs, milk, soy, and wheat. Government officials said that some 30,000 Americans are treated at hospital emergency rooms each year for allergic reactions to food, and as many as 250 die each year. Previously, ingredients such as whey and calcium caseinate may have been listed on a label rather than the more common term "milk." Similarly, lecithin had frequently been substituted for soy. Manufacturers also are required to disclose trans fat levels, which is said to contribute to elevated cholesterol levels and can lead to coronary artery disease. Food produced before the beginning of 2006 will be allowed to remain on the shelf without the new labels.

Source: http://tampabay.bizjournals.com/tampabay/stories/2006/01/09/ daily4.html?jst=b_ln_hl

[Return to top]

Water Sector

17. *January 08, Agence France−Presse* — **China hit by new toxic spill, water supply for millions threatened.** A fourth major toxic spill in China is threatening water supplies for millions of residents, officials and state media said, as local governments took emergency measures. In the eastern province of Shandong a diesel oil slick flowing down the Yellow River, China's second longest river, forced the province to stop pumping water from it, the Xinhua news agency said. So far 63 pumping stations along the river in several cities and counties, including the capital Jinan, have been shut down, said Xinhua. An official at the Jinan city Yellow River Affairs Bureau told Agence France−Presse the city of about six million people was now relying on water from reservoirs. The oil spill occurred Thursday, January 5, at Gongyi city in neighboring Henan province when a frozen pipe broke, causing six tons of oil to spill into a tributary of the Yellow River. The incident follows two spills of cadmium −− a chemical which can cause neurological disorders and cancer −− in the Xiangjiang River in Hunan province on January 4 and one in Guangdong province last month In November, a benzene slick from a factory explosion in northeast China polluted the Songhua River and cut tap water to millions of city−dwellers in Heilongjiang province.
Source: http://www.forbes.com/markets/feeds/afx/2006/01/08/afx243559 5.html

[Return to top]

Public Health Sector

18. *January 09, Reuters* — **China confirms latest human bird flu case.** China confirmed its eighth human infection from bird flu on Monday, January 9 the official Xinhua news agency said, revealing that a six−year−old boy had come down with the symptoms in December. The boy, surnamed Ouyang and from Guiyang county in the central province of Hunan, is undergoing treatment in hospital for the H5N1 strain of the virus. The H5N1 virus has killed more than 70 people since late 2003 and is endemic in poultry flocks across parts of Asia. China has suffered numerous outbreaks in poultry since October and Beijing has launched sweeping measures to stop the virus spreading and infecting more people, including a campaign to vaccinate all domestic poultry.
Source: http://www.alertnet.org/thenews/newsdesk/L09109845.htm

19. *January 09, International Herald Tribune* — **Reports of bird flu multiply in Turkey.** As a flurry of new reports of avian influenza in human beings and in animals emerged Sunday, January 8, from disparate parts of Turkey, international health officials said they now believed that the disease has been simmering in the eastern part of the country for months, even though it was only first reported there in late December. A team of experts, including specialists from the World Health Organization, accompanied by the Turkish Health Minister, was scrambling to determine the full extent of the outbreaks. Four children from villages near Van in Eastern Turkey have now been officially confirmed to have been infected with the H5N1 strain of the

disease by the World Health Organization, and at least 30 people are hospitalized in Van City as possible victims. A sibling of the two victims has also died, although tests for the virus so far have been negative. Turkish officials announced Sunday, January 8, that tests confirmed five more cases of H5N1, two in Van and three from around Ankara.
Source: http://www.boston.com/news/world/articles/2006/01/09/reports _of_bird_flu_multiply_in_turkey/

20. *January 05, Washington Technology* — **Centers for Disease Control passenger database raises concerns.** The U.S. Centers for Disease Control Prevention's (CDC) recent proposal to set up a new passenger database to track possible disease vectors and bioterrorism outbreaks may overlap with other databases, as well as raise privacy concerns, according to public comments submitted on the plan. The new database covers both airline and cruise ship passengers. The CDC's goal is to update regulations to reflect the potential for incoming air travelers to bring bird flu, Severe Acute Respiratory Syndrome and other emerging diseases into the U.S. The new proposed rule requires that passengers give emergency contact information, e−mail addresses, home addresses, names of traveling companions, and return flight information, among other data. Airline and cruise ship industries would have to collect the passenger information, maintain it electronically for at least 60 days and release it to CDC within 12 hours of a request. The airline industry is raising concerns about overlaps and what it considers to be inconsistent technical requirements between the new CDC database and airline passenger information collected for the Transportation Security Administration and Customs and Border Protection. The new provisions also call for observing passengers for signs of illness and specify symptoms that may make people subjected to quarantine, among other measures.
CDC analysis: http://www.cdc.gov/ncidod/dq/nprm/docs/draft_ria_final.pdf
Source: http://www.washingtontechnology.com/news/1_1/homeland/27692− 1.html

[Return to top]

Government Sector

21. *January 07, Pantagraph.com (IL)* — **Courthouse security procedures released.** New security cameras and procedures for public access to Illinois' DeWitt County courthouse have been released by county officials. The security plan will mean changes for employees who work in the county building. Identification cards have been issued to workers and must be used instead of keys to access areas of the building. Visitors accustomed to entering the back door of the courthouse for after−hours meetings also will notice changes. The new procedures require the public to pass through a security checkpoint located inside the Washington Street entrance. A sheriff's deputy will staff the security system during evening hours. According to DeWitt County Board Chairman Duane Harris, the board worked with DeWitt County Circuit Judge Stephen H. Peters on the project to screen all visitors and monitor areas of the building. The courthouse includes two courtrooms and offices related to the courts and the offices of the county clerk, treasurer, supervisor of assessments and other county offices. The $42,000 cost of updating the security system was shared between the county and Peters' office. The new equipment includes security cameras and computer−monitored access to the building. Harris said the cameras will help make security staff aware of problems before they are reported.
Source: http://www.pantagraph.com/articles/2006/01/07/news/103147.tx t

[Return to top]

Emergency Services Sector

22. *January 09, Federal Computer Week* — **National Oceanic and Atmospheric Administration puts technology to good use.** From development of quieter fishing vessels to tracking hurricanes, officials at the National Oceanic and Atmospheric Administration (NOAA) are effectively using technology to improve service to the country. For example, NOAA officials' plan to expand integration of aerial photography imagery with commercial services could help government agencies and insurance companies better assess damage from hurricanes, said Carl Staton, NOAA's chief information officer. Last fall, the agency partnered with Google to adapt aerial photography of damaged coastlines into the company's Google Earth application following Hurricane Katrina and other storms, Staton said. "You could pick out as one of the data parameters on Google Earth the NOAA damage assessment imagery and overlay it on their map," he said. "During our peak download time we were sustaining about a gigabyte per second in download of that imagery over several hours. Our peak download on any particular day was over 45 terabytes."
Source: http://fcw.com/article91884−01−09−06−Web

23. *January 06, Chicago Tribune* — **Chicago wants disaster readiness to be a part of every household.** Chicago launched an Internet−based emergency planning campaign Thursday, January 5, that officials said is designed to stress personal preparedness. Andrew Velasquez, executive director of Chicago's Office of Emergency Management, said it's crucial to make sure every resident is ready for a disaster −− from having a supply kit handy to knowing where to go for shelter. "The main objective is to make Chicago as prepared as any big city can be," Velasquez said. "Personal preparedness can mean the difference between life and death." The AlertChicago.com Website is the centerpiece of the campaign, which also includes brochures, pamphlets and announcements. Online, users can find instructions for emergencies ranging from extreme heat to outbreaks of disease to terrorism. The site also features a list of suggestions for disaster readiness and links to government agencies such as the Department of Homeland Security, the Federal Emergency Management Agency, and the state Emergency Management Agency.
Source: http://www.chicagotribune.com/news/local/chicago/chi−0601060238jan06,1,7182437.story?coll=chi−newslocalchicago−hed

24. *January 05, Computer World* — **District of Columbia rolling out service−oriented architecture for emergency response coordination.** The District of Columbia is poised to switch on a new system designed to allow emergency response command centers in Washington, DC, and surrounding areas to coordinate responses to natural disasters and terrorist attacks using Web services. The CapStat system, which will go live March 1, 2006, is built on a service−oriented architecture (SOA) that relies on Web services to allow emergency command centers in five jurisdictions in Washington, DC, Virginia, and Maryland to exchange information such as citizen reports of power outages, updated inventories of specific types of emergency response vehicles and the locations of people reporting suspicious disease symptoms. Paid for by a $1 million grant from the U.S. Department of Homeland Security, CapStat is relying on SOA to overcome system and data incompatibility problems associated

with retrieving and sharing data among the various jurisdictions.
Source: http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,107490,00.html?SKC=recovery−107490

[Return to top]

Information Technology and Telecommunications Sector

25. *January 09, Federal Computer Week* — **Federal Bureau of Investigation will focus on info sharing in 2006.** Sentinel, a case file system the Federal Bureau of Investigation (FBI) is developing, is one of several information technology projects getting under way in 2006, according to Zalmai Azmi, the FBI's chief information officer. The bureau started developing Sentinel in May 2005 after pulling the plug on the $170 million Virtual Case File (VCF) system. VCF was never deployed because of ongoing cost and schedule overruns. It was part of the FBI's Trilogy program to modernize the bureau's obsolete computer systems. Azmi said he would like to award the Sentinel contract in late January or early February. The first phase would start soon after and the second phase up to six months after the first. Ideally, the first phase would be complete 12 months after the contract is awarded, he said. Another initiative involves adding four Regional Data Exchanges (R−DExs) to the three that already exist. The R−DEx provides an interface that allows all levels of law enforcement to analyze complicated case file information and other data to fight terrorism and crime. The FBI also wants to create a National Data Exchange, which is an index to structured data at the federal, state and local levels.
Source: http://www.fcw.com/article91886−01−06−06−Web

26. *January 08, New Jersey.com* — **New Jersey law enforcement units combine to fight computer crime.** Three state law enforcement units in New Jersey will combine to fight computer crime. The new Computer Crime Task Force, formed by New Jersey state Attorney General Peter C. Harvey, will include personnel from the Division of Criminal Justice's (DCJ) Computer Analysis and Technology Unit (CATU), the New Jersey State Police Digital Technology Investigations Unit, and the state police Cyber Crimes Unit. The new task force will include three investigative units staffed with state troopers, DCJ investigators, and FBI special agents and will focus on computer hacking and viruses, Internet fraud, and the creation and distribution of child pornography. The Incident Response Unit investigations will focus on computers, computer networks, telecommunication devices, and other devices used in the commission of crimes. It will also provide cyber crime awareness outreach services to the public and train law enforcement regarding network intrusion crimes. The Cyber Crime Unit will investigate the use of computers in fraud and identity theft. A training committee will coordinate community outreach programs. The task force will aim to increase the reporting of cyber crime and computer intrusions. A Computer Crimes Task Force hotline is available at 1−888−648−6007, in addition to an online incident reporting form at http://www.cctf.nj.gov.
Source: http://www.nj.com/news/gloucester/local/index.ssf?/base/news−2/1136625344302990.xml&coll=8

27. *January 07, Security Focus* — **Apache mod_auth_pgsql multiple unspecified format string vulnerabilities.** Apache mod_auth_pgsql is prone to multiple format string vulnerabilities. Reports indicate that these issues could allow remote attackers to execute arbitrary code in the

context of the "apache" user and gain unauthorized access. Specific details of these vulnerabilities are not currently known.
Source: http://www.securityfocus.com/bid/16153/info

28. *January 06, Secunia* — **IBM Lotus Domino denial of service and unspecified vulnerabilities.** Some vulnerabilities have been reported in Lotus Domino, which potentially can be exploited by malicious users to cause a denial of service (DoS), or with unknown impact. Analysis is as follows: 1) Some unspecified potential security issues have been reported in "Agents"; 2) An unspecified boundary error in CD to MIME Conversion may cause a buffer overflow. This may be exploited to cause the router service to crash or become unresponsive; 3) A stack overflow error in Domino for AIX when evaluating a long formula in "Design" can potentially be exploited to crash Domino via an overly long recursive formula; 4) Some unspecified errors in the Directory Services can potentially be exploited to cause a DoS, e.g. via a crash when performing LDAP searches; 5) An unspecified error in the IMAP Server may cause the service to become unresponsive and unable to initiate new IMAP sessions; 6) An unspecified error may cause the server to crash when compact was executed from the client; 7) Several unspecified errors may cause the Web server to crash when handling corrupted bitmap images or when performing the "Delete Attachment" action.
Source: http://secunia.com/advisories/18328/

29. *January 06, Tech Web* — **Microsoft plans two more critical patches this week.** Microsoft may have released the Windows Metafile hot fix, but it has other patches still to come Tuesday, January 10, the Redmond, WA−based developer said late Thursday, January 5. In the monthly pre−patch notification it puts out five days prior to releasing fixes, Microsoft warned users that two security bulletins, both tagged as "Critical," will be issued Tuesday. In Microsoft's terminology, Critical means that a vulnerability can be remotely exploited. One of the two bulletins will involve Windows, and the other will affect Microsoft Office and Microsoft Exchange, the company's business suite and e−mail server software, respectively. Multiple non−security, high−priority updates will also be released Tuesday, as will an updated Windows Malicious Software Removal Tool. Microsoft will host a follow−up Webcast Wednesday, January 11, to answer questions about the fixes.
More details can be found in the advance notice posted on Microsoft's Website:
http://www.microsoft.com/technet/security/bulletin/advance.m spx
Source: http://www.techweb.com/showArticle.jhtml?articleID=175802037

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), 6881 (bittorrent), 445 (microsoft−ds), 27015 (halflife), 25 (smtp), 50079 (−−−), 3800 (−−−), 139 (netbios−ssn), 135 (epmap), 32801 (−−−) 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.