Department of Homeland Security Daily Open Source Infrastructure Report for 17 January 2006

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

Daily Highlights

- USA TODAY reports the Federal Trade Commission has unveiled an online tool designed to help consumers avoid becoming victims of Internet scams. (See item 9)
- The Associated Press reports an Alaska Airlines passenger jet had to make an emergency return to Seattle−Tacoma Airport after a company mechanic apparently left a landing−gear door open. (See item 14)
- CNN reports the Department of Homeland Security has asked the nation's truckers to help find a man who has been seen taking photographs of tanker equipment as well as asking truck drivers several questions about deliveries and operations. (See item 16)

DHS Daily Open Source Infrastructure Report *Fast Jump*

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 14, Associated Press* — **Expensive, volatile gas has Florida looking for alternative fuel.** Florida Governor Jeb Bush has been talking about burning sugar cane waste. In a few counties, they're capturing and using the methane produced by rotting garbage in landfills. And Progress Energy and Florida Power and Light are both planning to increase production of nuclear power. The biggest percentage of Florida's electricity is made using natural gas. But the

shock of last year's huge run−up in prices, and the interruption of the gas supply after Hurricane Katrina has Bush and other state officials urgently trying to find different ways to make electricity. Bush said the price increases, which were spurred by worldwide demand but exacerbated by hurricanes that disrupted production in the Gulf of Mexico, made it clear the state needs to rely on it less. "We need diversity of supply," Bush said last month addressing an energy summit on the future of Florida's electric supply. Bush said conservation is a key part of the solution too, and is doing what he can. Last year he ordered state buildings to dim the lights and turn down the air conditioning to help save electricity. He's also proposing incentives for alternative fuel production.
Source: http://www.sun−sentinel.com/news/local/southflorida/sfl−flor idaenergyfuture−jan14,0,4710995.story?coll=sfla−home−headlin es

2. *January 14, Associated Press* — **Oil prices fall, markets fret about Iran.** Crude oil futures fell marginally on Friday, January 13, ending the week slightly lower as above−normal temperatures in parts of the U.S. helped ease supply concerns. But the market remained worried about oil−rich Iran, which threatened to block inspections of its nuclear sites if confronted by the United Nations Security Council. Also on Friday, Iran, the world's fourth−largest oil producer, vowed to end all voluntary cooperation with the UN nuclear watchdog if it is referred to the Security Council for possible sanctions over its controversial nuclear program. Balmy weather in the U.S. Northeast, a key heating oil market, helped offset those geopolitical concerns. Heating oil and natural gas prices have been under pressure due to U.S. government reports hinting at weak demand last week. The latest federal data show that 18 percent of daily natural gas production in the Gulf of Mexico remains shut, and that 26 percent of daily oil output is still down.
Source: http://www.casperstartribune.net/articles/2006/01/14/ap/busi ness/d8f40fao4.txt

3. *January 14, Baltimore Sun (MD)* — **Baltimore Company plans gas terminal.** Arlington, VA−based power supplier AES Corp. says it wants to build a $400 million liquefied natural gas terminal on the site of the former Sparrows Point shipyard in Baltimore County, joining a nationwide push among power companies to increase gas imports in the face of domestic shortages and rising prices. The proposed project, which is still in preliminary discussions, would include a marine terminal, storage tanks and an 85−mile pipeline that would cost an additional $200 million to $250 million and connect to an existing natural gas distribution center in suburban Philadelphia. But AES will have to persuade environmentalists and Baltimore County residents to sign off on the plan at a time when similar projects have met with stiff resistance along the East Coast. Opponents in other communities have raised concerns such as tanker spills and terrorist attacks that could cause explosions and imperil nearby residents. Power companies have proposed to build 40 similar terminals in North America as the nation deals with a growing energy shortage that was highlighted when hurricanes last year cut off production in the Gulf of Mexico. It's estimated that about a dozen will be constructed.
Source: http://www.baltimoresun.com/business/bal−te.bz.lng14jan14,1, 4505880.story?coll=bal−home−headlines&ctrack=1&cset=true

4. *January 12, Energy Central News* — **California PUC approves nation's biggest solar program.** The California Public Utilities Commission (CPUC) on Thursday, January 12, approved the California Solar Initiative, a program to install 3,000 megawatts of solar on California homes, businesses, farms, schools and public facilities over 11 years. The initiative is

the nation's largest solar power investment, designed to make solar power mainstream and affordable. It will add clean energy to the state's peak demand resources, reduce risk by diversifying the state's energy portfolio, and establish a world−class solar market in California. The California Solar Initiative creates 11 years of funding for consumer rebates. The CPUC will provide $2.8 billion in customer incentives for solar projects on existing residential buildings, as well as all public buildings, industrial facilities, businesses, and agricultural facilities. The historic initiative will provide the power equivalent of six large natural−gas fired power plants, while reducing the need for costly updates to California's congested electric grid. According to a staff report prepared by the CPUC in the summer of 2005, the state's investment in solar power will save California ratepayers billions of dollars net of incentives over system lifetimes. These energy savings come at a critical time for California consumers, as record−level natural gas prices continue to add to citizens' heating and electric bills. Source: http://www.energycentral.com/centers/news/daily/article.cfm? aid=6232425

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *January 13, Washington Post* — **Army ends Lockheed contract for new spy plane.** The Army canceled its contract for a new spy plane Thursday, January 12, after the Lockheed Martin Corp. program developed technical problems that military officials determined were too expensive to fix. Bethesda, MD−based Lockheed, the nation's largest defense contractor, spent months trying to save the plane, known as the Aerial Common Sensor, which was supposed to detect enemy signals and track enemy troop movements from 37,000 feet in the air. But Lockheed struggled to fit all of the required technology on the aircraft it picked for the job. "After carefully evaluating Lockheed's proposals [to save the program], we decided that the prudent course of action at this time was to terminate the contract," Claude M. Bolton, the Army's acquisition chief, said in a written statement. In a letter to Congress, the Army said it would open a new competition for the plane in 2009. The Pentagon will begin a six−month study of its intelligence, surveillance and reconnaissance aircraft, the Army letter to Congress said. The planes that the Aerial Common Sensor was to replace, the Army's Guardrail Common Sensor and Airborne Reconnaissance Low and the Navy's EP−3E, will continue to operate. Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/12/AR2006011201536.html

6. *January 09, Journal of Net−Centric Warfare* — **U.S. Congress asserts oversight of FCS program, trims budget.** U.S. lawmakers have asserted much greater oversight into the Army’s mammoth Future Combat Systems (FCS), demanded better reporting on the program’s progress and trimmed $240 million from the service’s $3.4 billion request for the program in 2006. The cut was a compromise between the Senate, which wanted to fully fund the program, and the House, which sought to cut $400 million. The changes will become law with the expected

signing of the 2006 Defense Authorization Act. Launched in 1999, the $161 billion FCS is history's most expensive land−warfare program. The Army has argued that FCS should be funded by a single pool of money, which service leaders distribute among various program elements. But Congress, never fully convinced of FCS' value for money, has balked as projected costs rose from the Army's initial estimate of $92 billion. Lawmakers said the Government Accountability Office now must provide annual reports on how well FCS is meeting its original goals and current and future budget requests. The authorization bill directs that in 2008, FCS must be broken up into six separate program elements: Manned Ground Vehicles; Systems of Systems Engineering and Program Management; Reconnaissance Platforms and Sensors; Unmanned Ground Vehicles; Unattended Sensors; and Sustainment.
Source: http://www.isrjournal.com/story.php?F=1457751

[Return to top]

Banking and Finance Sector

7. *January 13, CNET News* — **UK banks off the hook for Indian data breach.** British banks will not face any action over an alleged data breach in an Indian call center last year, the UK's data protection watchdog has said. In the breach, an undercover newspaper reporter was allegedly able to buy the bank account, credit card, passport and driving license details of 1,000 British bank customers for just $7.50 each from a New Delhi call center worker who was said to have promised to supply confidential data from 200,000 accounts per month. The Information Commissioner (IC), the UK's data protection agency, warned at the time that the banks could face prosecution for a criminal breach of the country's Data Protection Act. But the IC said on Friday, January 13, that it will not be taking action against any of the banks involved in the newspaper sting. Following an investigation, there was no evidence that any personal information was compromised, it said.
Source: http://news.com.com/U.K.+banks+off+the+hook+for+Indian+data+breach/2100−1029_3−6027073.html?tag=cd.top

8. *January 12, IDG News* — **FBI warns of mining accident e−mail scam.** The U.S. Federal Bureau of Investigations (FBI) is warning Internet users to be on the look out for a fraudulent e−mail soliciting money for a survivor of a mine accident in the U.S. last week. The e−mail purports to be written by a doctor at the hospital where the miner is being treated and describes the condition of the survivor and the financial assistance that is needed for a full recovery. "The FBI takes these matters seriously and is working with other law enforcement and private industry partners to identify the person(s) responsible," the agency said in a statement on Wednesday, January 11. "Anyone who has received an e−mail of this nature is asked to contact the FBI's Internet Crime Complaint Center via the Website at www.ic3.gov." The bureau also repeated its standard advice to refrain from opening or responding to unsolicited e−mails and to verify thoroughly any requests for money or personal information received via e−mail before responding.
Source: http://www.networkworld.com/news/2006/011106−mining−accident .html

9. *January 10, USA TODAY* — **Federal Trade Commission launches site to fight cybercrime.** Responding to the rising cybercrime threat, the Federal Trade Commission (FTC) on Tuesday, January 10, unveiled an online tool designed to help consumers avoid becoming victims of

Internet scams. At the Website, consumers can take interactive quizzes designed to enlighten them about ID theft, phishing, spam and online−shopping scams. If the user selects a wrong answer, the program explains why that particular misconception about Internet security can lead to trouble. Elsewhere on the site, consumers can find detailed guidance on how to monitor their credit histories, use effective passwords and recover from identity theft. "We're trying to make the information as accessible as possible, with tips so people can take action," said Nat Wood, the FTC's assistant director for consumer and business education. The education push comes as the tide of cybercrime continues to rise. Five federal agencies and 13 private organizations partnered to sponsor the OnGuard Online Website. Information on the site is not copyrighted, and the FTC encourages companies and other organizations to download and widely disseminate the information.
Website: http://www.onguardonline.gov
Source: http://www.usatoday.com/money/perfi/general/2006−01−10−ftc−u sat_x.htm

[Return to top]

Transportation and Border Security Sector

10. *January 16, Associated Press* — **Suspicious item prompts evacuation of section of San Francisco terminal.** Part of a San Francisco International Airport terminal was evacuated for several hours Sunday, January 15, after a suspicious item was found in a piece of luggage, officials said. A baggage screener in the American Airlines section of Terminal 3 "noticed a suspicious item" in a passenger's carryon bag shortly before 1 p.m. PST said airport spokesperson Mike McCarron. Authorities would not say what exactly was found in the bag, but San Francisco police Lt. Bill Darr said, “there were items, articles inside the carryon luggage that did resemble components of a possible device.” Authorities later found that there were no explosives in the bag, said airport duty manager Bob Schneider. Two men and a woman connected to the luggage were held for questioning and later released, authorities said. The immediate area around the security checkpoint was evacuated and at least seven afternoon flights were delayed as a bomb squad investigated, Schneider said.
Source: http://www.usatoday.com/travel/news/2006−01−16−sfo−evac_x.ht m

11. *January 16, Associated Press* — **Plane makes emergency landing in Philadelphia.** A US Airways plane was forced to shut down one of its two engines and make an emergency landing at Philadelphia International Airport on Sunday, January 15, authorities said. Flight 4455, a twin−engine turboprop, declared an emergency about 20 minutes after taking off from the Philadelphia airport bound for Baltimore−Washington International Airport, US Airways spokesperson Carlo Bertolini said. "One of the engines was shut down," he said. The plane, carrying 48 passengers and three crewmembers, returned to Philadelphia, landed at about 4:50 p.m. EST, and was towed to the gate.
Source: http://www.usatoday.com/travel/news/2006−01−16−philly−landin g_x.htm

12. *January 15, Associated Press* — **Inspectors say questionable aircraft parts are okay.** Alaska Airlines inspectors in Seattle have found 15 cases of "dry" jackscrews on MD−80 series jets since March 2003. But in a report released Friday, January 13, by the airline, the Federal Aviation Administration (FAA) said a dry jackscrew does not necessarily indicate that it is unsafe or has not been properly lubricated. The FAA report found "no safety issues" and said

the "overall risk for jackscrews is low." The two−foot−long jackscrew is a key component in the tail of the MD−80 series jet. It moves the horizontal stabilizer at the top of the jet's tail, helping to control the plane in flight. In January 2000, Alaska Airlines Flight 261 crashed off the coast of California when the jackscrew failed on a flight from Mexico to Seattle. After a long investigation the National Transportation Safety Board ruled that the jackscrew had not been lubricated. The board criticized Alaska for poor maintenance practices and the FAA for lack of oversight.
Source: http://www.katu.com/news/story.asp?ID=82530

13. *January 13, Reuters* — **U.S. airline pilots complaining more about fatigue.** A growing number of U.S. airline pilots are complaining about fatigue from longer work days brought on by crew schedule changes at airlines that have restructured, or continue to restructure in bankruptcy, the nation's top pilots' union said Thursday. The Air Line Pilots Association also said at least one airline, JetBlue Airways, is pressuring regulators for an exemption to federal limits on crew time, especially on long−haul flights. JetBlue says it would like more flexibility to improve quality of life for pilots, not for economic reasons. About half of JetBlue's 355 daily flights are long−haul service. The union represents aviators at the biggest airlines that have sought bankruptcy since 2002 −− United Airlines, US Airways, Northwest Airlines and Delta Air Lines as well as some smaller carriers. Regulations limit pilots to eight hours of flying time on domestic service in any 24−hour period. But actual work days negotiated in union contracts −− including flight preparation and airport down time −− were usually capped around 16 hours. In reality, thousands of ALPA pilots at struggling carriers worked less than 14 hours daily until their companies gutted contracts and sought more productivity in bankruptcy to compete better with nimble low−cost rivals.
Source: http://www.usatoday.com/travel/news/2006−01−13−pilot−fatigue_x.htm

14. *January 13, Associated Press* — **Landing−gear door left open on Alaska Airlines flight.** An Alaska Airlines passenger jet had to make an emergency return to Seattle−Tacoma International Airport after a company mechanic apparently left a landing−gear door open, the company has acknowledged. It happened on Wednesday afternoon, January 11, after the pilot of Flight 536 asked mechanics to fix a broken taxi landing light. The open door caused vibrations strong enough for passengers to take notice immediately after takeoff. The MD−80 jet landed safely at Sea−Tac at 4:36 p.m. PST, 16 minutes after it departed, Alaska spokesperson Amanda Tobin said. The landing−gear door on the MD−80 is normally closed. It opens briefly when the pilot retracts the landing gear after takeoff, and again when the pilot deploys the landing gear before the plane touches down. Port of Seattle fire trucks and emergency vehicles were standing by when the jet landed, at the pilot's request, airport spokesperson Bob Parker said. It's the latest in a string of incidents involving Alaska Airlines planes.
Source: http://www.usatoday.com/travel/news/2006−01−13−alaska−air−in cident_x.htm

15. *January 13, Department of Homeland Security* — **E−Passport testing begins at San Francisco International Airport.** A live test of e−Passports, that contain contactless chips with biographic and biometric information and the readers that are capable of reading these e−Passports, began January 15, 2006 at Terminal G at San Francisco International Airport (SFO). This test is a collaborative effort between the United States, Australia, New Zealand, and Singapore that will run through April 15, 2006. Participants include citizens of Australia and New Zealand who have been issued the new e−Passports, Singapore Airlines crew and

officials holding trial e−Passports, and U.S. diplomatic and official e−Passport holders. The test will assess the operational impact of using new equipment and software to read and verify the information embedded in the e−Passports. Participants will present their e−Passports when arriving in the United States at SFO, at Changi Airport in Singapore, or at Sydney Airport in Australia. The e−Passport contains the holder's biographic information and a biometric identifier, in this case a digital photograph, embedded in a contactless chip set in the passport. The inspection process for those participating does not change. The goal of the live test is to gather information that can support countries around the world in their development and implementation of e−Passports that comply with International Civil Aviation Organization standards.
Source: http://www.dhs.gov/dhspublic/display?content=5342

16. *January 12, CNN* — **Alert: Man photographed trucks, tankers.** The Department of Homeland Security has tapped the nation's truckers to help find a man who has been seen taking photographs of tanker equipment. On three separate occasions, the man also asked truck drivers several questions about deliveries and operations, according to the Highway Information Sharing and Analysis Center. "The individual in question is also reported to have videotaped tank truck operations and deliveries as well as taken photographs of tanker equipment," states the "Be on the Lookout," or BOLO, alert. "Law enforcement has requested assistance in ascertaining the identity or whereabouts of the person in question." Officials say the man has short, dark, wavy hair and a dark complexion. He is in his early 50s, and truckers who have spoken to him say it sounds like English is his second language. The alert describes three incidents that raised concern: one in Fort Myers, FL, in April; another in Tampa, FL, in May; and another in Ringgold, GA, in 2004. The same man is believed to be involved in all three incidents. There have been similar, more recent incidents, but it's not clear whether they involve the same man. Though the BOLO request was made public this week, several bulletins have gone out to law enforcement officials in the last eight months.
Source: http://www.cnn.com/2006/US/01/12/trucker.lookout/index.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *January 16, Wisconsin Ag Connection* — **Authorities investigating fence cutting at chronic wasting disease infected farm.** State wildlife officials are looking into why the perimeter fence was cut at a Portage, WI, deer farm, which was infected with chronic wasting disease (CWD) several years ago. According to the Wisconsin Department of Natural Resources (DNR), it is still unknown when the fence was cut or if any deer are missing at Buckhorn Flats near Almond. "This was not an accident. There was roughly a three−foot−square area of the woven wire fence cut and wired back to form an opening, " said DNR CWD Project Leader Alan Crossley. Crossley says DNR staff have begun shooting deer outside the fence Friday, January

13, which will be tested for CWD. About 40 bucks are in the hunting preserve, based on earlier statements from the owner. Deer in preserves roam free over a large fenced−in area, rather than being in pens, so it is difficult to get a detailed count. There are about 79 does, fawns, and yearling bucks fenced in smaller breeding pens on the farm. The fence around that area was not breached.
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=54&y r=2006

18. *January 15, Associated Press* — **Hawaii serves as world's biotech lab.** Since 1988, federal regulators have approved more than 10,600 applications to grow experimental biotech crops on 49,300 separate fields throughout the U.S. More of these are in Hawaii than any other state. Through the powers of biotechnology, low−nicotine tobacco, disease−resistant cotton, and soy immune to weed killer are grown there. Hawaii's genetically engineered corn projects outnumber even those grown in Iowa and Illinois. In many ways, the biotechnology debate in Hawaii is a microcosm of the global debate over biotechnology. There hasn't been a single allergic reaction or other health problem credibly connected to consuming biotech food. Still, many scientists do worry about the threats biotechnology poses to the environment, mainly through inadvertent cross−pollination with conventionally grown crops. The industry and its supporters point out that biotechnology is actually helping small farmers by reducing pesticide use. In Hawaii, several anti−biotech measures have been introduced recently in the Legislature mimicking laws in four California counties banning biotech, though none have passed so far.
Source: http://msnbc.msn.com/id/10841731/

19. *January 13, Stop Soybean Rust Now* — **First soybean rust of year found in Alabama.** The first soybean rust of 2006 was detected on two kudzu patches in the city of Montgomery, AL, Thursday, January 12. Montgomery is approximately 125 miles north of the Florida Gulf Coast. According to Ed Sikora, professor and Extension plant pathologist with Auburn University, most of the two patches were dormant, but the remaining green foliage was infected with the disease. One patch was in a protected site on the north side of an underpass off of Interstate 85, while the other patch was hanging in a tree along a bluff of the Alabama River. This is the first report of soybean rust in Montgomery County. Soybean rust has been detected in 34 counties in Alabama since June 2005. There were 138 U.S. counties found to have soybean rust in calendar year 2005. This is the first reported U.S. rust find in the new year.
Source: http://www.stopsoybeanrust.com/viewStory.asp?StoryID=670

20. *January 13, U.S. Department of Agriculture* — **Funds awarded to sequence swine genome.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns announced Friday, January 13, that USDA is awarding $10 million to the University of Illinois to obtain a draft sequence of the swine genome. "Pork is the major white meat consumed worldwide," Johanns said. "With more than 61 million pigs in the nation, the sequence of the pig genome will have a significant impact on U.S. agriculture." The two−year project will lead to the development of new DNA−based tools to identify and select genetically superior pigs that resist infectious diseases, yield larger litter sizes, and produce leaner cuts of meat for consumers. Several other institutions are collaborating with the University of Illinois, including: Roslin Institute, Edinburgh, Scotland; University of Nevada, Reno; Wellcome Trust Sanger Institute, United Kingdom; INRA Cellular Genetics Laboratory, Toulouse, France; USDA Agricultural Research Service Meat Animal Research Center, Clay Center, NE; and Iowa State University.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?conten

tidonly=true&contentid=2006/01/0005.xml

21. *January 12, Animal and Plant Health Inspection Service* — **Proposal to amend tuberculosis regulations for re−accreditation test for captive cervids.** The U. S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) is proposing the following amendments to regulations regarding bovine tuberculosis (TB) in captive cervids: increasing, by one year, the term for which accredited herd status is valid; to allow re−accreditation tests to be performed within 33−39 months of the anniversary date and removing references to the blood TB test. APHIS also is proposing to reduce, from three tests to two, the number of consecutive negative official TB tests. These tests are required of all eligible captive cervids in a herd before the herd can be eligible for recognition as being accredited. Amending the regulations to extend the period between re−accreditation tests, as well as reducing the number of consecutive negative, official TB tests, will reduce testing costs for herd owners, lessen the potential for animal injury or death during testing, and lower administrative costs for state and federal regulatory agencies. Bovine TB is a contagious and infectious disease caused by Mycobacterium bovis. It affects cattle, bison, deer, elk, goats, and other warm−blooded species. Source: http://www.aphis.usda.gov/newsroom/content/2006/01/tbregs.sh tml

[Return to top]

Food Sector

22. *January 16, USAgNet* — **European panel approves enhanced corn.** The European Commission Friday, January 13, announced that it has approved the use of Monsanto's YieldGard Rootworm corn (MON 863) and its processed products as food and food ingredients under the Novel Foods Regulation. With this announcement, the European Union (EU) authorizes the immediate use of YieldGard Rootworm for human consumption. today's decision is expected to be published in the Official Journal of the European Communities in the coming weeks. In addition, the EU Commission also granted import feed and processing approval of YieldGard Plus, which is a hybrid stack of YieldGard Rootworm (MON 863) with YieldGard Corn Borer (MON 810). YieldGard Plus is currently under review by the EU for use in food and food ingredients. The European Commission's ruling does not include the approval of YieldGard Rootworm corn or YieldGard Plus for cultivation in the EU or the import approval for any YieldGard Rootworm combined trait products. YieldGard Rootworm corn contains a protein from Bacillus thuringiensis (Bt −− a common soil microbe) that specifically targets corn rootworm larvae, allowing the corn plant to naturally protect its roots against the damaging corn rootworm. The U.S. Department of Agriculture estimates that this pest causes one billion dollars in lost revenue annually to the U.S. corn crop.
Source: http://www.usagnet.com/story−national.cfm?Id=61&yr=2006

23. *January 14, Associated Press* — **Korea to allow some U.S. beef.** South Korea agreed Friday, January 13, to resume shipments of U.S. beef, which had been prohibited since the December 2003 discovery of mad cow disease in the U.S. But senior U.S. officials pressed South Korea to lift some of the conditions that will continue to keep out almost half of traditional American beef exports. South Korea continues to prohibit ribs and other bone−in beef, which keeps closed about 45 percent of the potential market. South Korea was worth $815 million to U.S. producers in the year before the ban. The country once was the third−biggest customer of

American beef behind Japan and Mexico.
Source: http://www.dfw.com/mld/dfw/news/13626478.htm

[Return to top]

Water Sector

24. *January 12, Associated Press* — **Arizona could have its driest winter season in centuries.** As much of Arizona enters an 11th year of drought conditions, the state could experience its driest winter season in centuries. Arizona's mountains are virtually bare, with snowpack conditions worse than they were at the same time in 2002 −− a year that set records as one of the driest in five centuries. Rural areas are bracing for water shortages by early summer if rains don't come. January and February typically bring much of the snow needed to refill reservoirs and keep rivers and forests healthy. But a stubborn weather pattern has been steering every storm north of Arizona so far this winter. The Salt and Verde rivers' watersheds received just 0.14 of an inch of rain in November and December, and none has fallen in Phoenix since October 18. The state Department of Water Resources has begun meeting with local leaders under a drought plan produced two years ago by a governor's task force. That process, led in part by a newly appointed statewide drought coordinator, is expected to take on added importance as rural communities seek guidance in creating drought and conservation blueprints.
Source: http://www.usatoday.com/weather/climate/2006−01−12−arizona−d rought_x.htm

[Return to top]

Public Health Sector

25. *January 16, Reuters* — **Indonesian girl dies of bird flu, local test shows.** A 13−year−old Indonesian girl died of bird flu at the weekend while two others from her family have tested positive for the H5N1 virus, a health ministry official said on Monday, January 16, citing the results of local tests. If confirmed by outside laboratories recognized by the World Health Organization, the case would take total known deaths in Indonesia from the avian flu to 13 and the number who have had bird flu to 20. "We found three positive bird flu cases in one family coming from Indramayu, West Java," the official, Hariadi Wibisono, said. He said the girl died in an Indramayu hospital while her 15−year−old sister and 3−year−old brother had been sent for treatment at a hospital in Jakarta designated to treat bird flu patients. "A lot of fowls died around the neighborhood where they lived. But we don't know yet whether these fowls were carrying the virus. We sent a team there to investigate this morning."
Source: http://today.reuters.com/news/newsArticle.aspx?type=worldNew s&storyID=2006−01−16T032756Z_01_SP237235_RTRUKOC_0_US−BIRDFL U−INDONESIA.xml&archived=False

26. *January 15, Agence France−Presse* — **British investigators seize massive haul of suspected stolen bird flu drug.** British investigators have seized an estimated 500,000 stg haul of a suspected stolen batch of the anti−viral drug Tamiflu, which is manufactured by Swiss pharmaceuticals company Roche Holding AG. Officers from the government's Medicines and Healthcare Products Regulatory Agency (MHRA) carried out a raid at an undisclosed address

in London Wednesday, January 11, and confiscated 5,000 packets of the drug. Results of tests on the batch, which was being sold on the Internet, are expected in the next two weeks, an MHRA spokesperson said, but signs were the drug −− believed to be the most effective against bird flu −−was genuine. The MHRA probe is part of an international crackdown on the trade in either fake or black market Tamiflu across Europe and beyond.
Source: http://www.forbes.com/work/feeds/afx/2006/01/15/afx2450802.h tml

27. *January 15, Agence France−Prese* — **Girl dead of suspected bird flu tests negative, brother confirmed with virus.** Initial tests on a 12−year−old girl who died of bird flu−like symptoms in Van, Turkey, are negative for the H5N1 strain of the virus, but her five−year−old brother has tested positive, the health ministry announced. Tests on Muhammed Ozcan, whose sister Fatma died Sunday, January 15, at the Van University Hospital, came back positive, the ministry said in a statement. "The preliminary tests on Fatma are negative, however," said the document, which added that other tests would be carried out. Fatma's case recalled that of another child, 11−year−old Hulya Kocyigit, one of three siblings from the eastern town of Dogubeyazit to have died from avian influenza. Experts initially said Hulya's brother and sister, aged 14 and 15, had tested positive for H5N1, but she had not −− further tests revealed bird flu as the cause of her death several days later. Muhammed became the 19th person, including the three who have already died, to be infected by the disease in Turkey and outside eastern Asia, where nearly 80 people have died since 2003. The current outbreak emerged in Dogubeyazit in late December and spread across the country. It has now been reported in nearly a third of Turkey's 81 provinces.
Source: http://news.yahoo.com/s/afp/20060115/hl_afp/healthfluturkey_060115164540

28. *January 14, U.S. Centers for Disease Control and Prevention* — **CDC recommends against the use of two drugs for the treatment of influenza.** While the primary strategy for preventing complications of influenza infections is annual vaccination, antiviral medications with activity against influenza viruses can be effective for the prophylaxis and treatment of influenza. Two classes of antivirals are currently available—the M2 ion channel inhibitors (i.e., the two adamantanes amantadine and rimantadine) and the neuraminidase inhibitors (i.e., oseltamivir and zanamivir). The neuraminidase inhibitors are effective for the treatment and prophylaxis of influenza A and B, while the adamantanes are only active against influenza A viruses. This alert provides new information about the resistance of influenza viruses currently circulating in the U.S. to the adamantanes, and it makes an interim recommendation that these drugs not be used during the 2005–06 influenza season. The U.S. Centers for Disease Control and Prevention (CDC) is providing an interim recommendation that neither amantadine nor rimandatine be used for the treatment or prophylaxis of influenza A in the U.S. for the remainder of the 2005–06 influenza season. During this period, oseltamivir or zanamivir should be selected if an antiviral medication is used for the treatment and prophylaxis of influenza.
Source: http://www.cdc.gov/flu/han011406.htm

29. *January 13, Washington File* — **New Ebola therapy protects animals from lethal disease.** Scientists at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) in Maryland have developed a successful strategy for interfering with Ebola virus infection that protected 75 percent of rhesus monkeys exposed to the lethal disease. This is the first successful anti−viral intervention against RNA filoviruses like Ebola in monkeys. The findings could serve as the basis for a new approach to developing quickly virus−specific therapies for known,

emerging, and genetically engineered pathogens. "One advantage of this strategy is that it directly targets the virus," said Kelly Warfield, one of the study authors. "With Ebola infection, the virus grows so fast that it overtakes the host immune system," he added. "What we did, essentially, was to hold off the viral replication long enough for the host to mount an immune response and clear the virus." The term filo means "threadlike" in Latin. Filoviruses −– among the most lethal and destructive known −– cause viral hemorrhagic fevers, characterized by massive bleeding from every opening in the body. The Ebola virus is infectious by transmission through the air, although it is more commonly spread through blood and bodily fluids. It is a global health threat and a potential agent of biological warfare or terrorism.
Ebola information: http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/ebola.ht m
Source: http://usinfo.state.gov/xarchives/display.html?p=washfile−en glish&y=2006&m=January&x=20060113160459lcnirellep0.206535&t= livefeeds/wf−latest.html

[Return to top]

Government Sector

30. *January 16, Herald Net (WA)* — **Judging courthouse safety.** On a typical business day, up to thousands of visitors funnel through a narrow security screening area at the east entrance of Washington's Snohomish County Courthouse. Contract security workers use an X−ray machine to check bags, umbrellas and other packages. People walk through a metal detector so that weapons, or things that could be used as weapons, are not carried into the building. The technology should assure visitors and workers that they are safe inside. But Snohomish County judges and administration want to be sure. That's why a consultant was hired to study security procedures at the courthouse in downtown Everett and at the Denney Juvenile Justice Center in north Everett to determine if changes are wise. The question of security screening itself surfaced in Everett and elsewhere in Washington in 1995 after a man carried a pistol into the King County Courthouse, confronted his pregnant wife outside a divorce court and shot her and two of her friends to death. Persistent security concerns include having too few marshals available in the courthouse, and allowing courthouse employees to use separate entrances to get into the building without screening, Superior Court Administrator Dick Carlson said.
Source: http://heraldnet.com/stories/06/01/16/100loc_a1courtsecure00 1.cfm

[Return to top]

Emergency Services Sector

31. *January 15, The Courier (IA)* — **Iowa officials hold emergency response drill.** A simulated explosion on the Wartburg College campus in Waverly, IA, Saturday, January 14, tested Bremer County's emergency response system. In the scenario, about 20 victims were injured or killed in an explosion. Wartburg security, Waverly police, Waverly Fire Department and services from Janesville, Denver, Tripoli, Frederika, Shell Rock and Plainfield participated. Waverly Health Center also tested its ability to handle a surge of patients as victims. From start to finish it took the 70 rescue personnel about one hour to clear the library building of injured and dead victims. Immediately following the drill, rescue personnel met to discuss

performance. Waverly police department Sgt. Gary Rieck discovered areas of campus where he could not receive radio communications. Other personel discovered weaknesses of interagency communications. Kip Ladage, Bremer County Emergency management coordinator, said the next step will be to take the information and discuss how they could improve disaster response. One improvement might be to reprogram radios or even buy new communications equipment. Wartburg Communications Arts Department members video recorded the exercise and will create a training video for firefighters and ambulance crew.
Source: http://www.wcfcourier.com/articles/2006/01/15/news/metro/f50ae73972a7fb44862570f70015f25a.txt

[Return to top]

Information Technology and Telecommunications Sector

32. *January 14, Security Focus* — **Cisco IP Phone 7940 remote denial of service vulnerability.** Cisco IP Phone 7940 is prone to a remote denial of service vulnerability. Cisco has released a security notice to address this issue. Version 7.1(1) firmware for affected devices are now capable of throttling incoming connections, and will not reset themselves when attacked. Please see the referenced advisory for further information on obtaining fixed firmware.
Cisco Security Notice: http://www.cisco.com/warp/public/707/cisco−response−20060113−ip−phones.shtml
Source: http://www.securityfocus.com/bid/16200/references

33. *January 14, Washington Post* — **Iraqi telecom chief seeks to build from scratch.** The Iraqi telecom system was one of the most rudimentary in the Middle East under Saddam Hussein, with roughly one million land lines for a population of about 26 million and no mobile−phone networks. Today, the Iraqis are trying to leapfrog generations of technology by going straight to an advanced wireless phone system. According to Siyamend Z. Othman, Iraq's top telecommunications regulator, there are between four million and four and a half million mobile−phone subscribers, up from zero when the U.S.−led invasion began nearly three years ago. According to U.S. estimates, the number of landlines, which fell by several hundred thousand because of U.S. bombing, now slightly exceeds the prewar level. Setting up cell towers is cheaper and easier than rolling phone lines to every home in Iraq, which has three main mobile providers −− all regional, rather than Western, companies −− working overtime. One saving grace that the new telecom infrastructure has largely been spared insurgent attacks for a simple reason: The terrorists want phone service, too. Othman said that what he needs most are trained professionals as the government works to provide service to a population starved of communications under Hussein.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/13/AR2006011301747.html

34. *January 13, Register (United Kingdom)* — **Anti−spyware group defines detection guidelines.** The Anti−Spyware Coalition (ASC), an alliance of software companies, security firms and consumer organizations, has agreed a set of guidelines on detecting invasive finalized spyware. The final draft of the ASC's "risk−modeling description" aims to give an objective criteria on whether a program is malign. A draft of this description was thrown open for public comment in October and the final version that's emerged is essentially an expanded and polished version.

The group defines spyware and other potentially unwanted technologies as deployed without appropriate user consent and/or implemented in ways that impair user control over: material changes that affect their user experience, privacy, or system security; use of their system resources, including what programs are installed on their computers; and/or collection, use, and distribution of their personal or other sensitive information. In addition, ASC finalized the list of speakers for its first public meeting which is due to take place on Thursday, February 9, at the Hyatt Capitol Hill in Washington, DC. Federal Trade Commission (FTC) Chairman Deborah Platt Majoras will keynote at the single day event, which will also feature federal regulators, and top state technology and law enforcement officials.
Source: http://www.theregister.co.uk/2006/01/13/anti_spyware/

35. *January 13, New York Times* — **Federal agency shuts down contractors site.** The General Services Administration (GSA) has shut a Website for government contractors after a computer industry consultant reported that he was able to view and modify corporate and financial information submitted by vendors. The security flaw, which could have permitted contractor fraud, was reported to the agency's inspector general on December 22, but almost three weeks passed before the system was taken offline Wednesday afternoon, January 11. The GSA is the federal agency responsible for procuring equipment and services, including computer security technology, making the lapse all the more striking. The agency said it believed that the flaw had not been exploited by intruders or by authorized users. It is not clear how long the problem existed. The Website, called eOffer, was introduced in May 2004 to let companies respond electronically to requests for proposals for computer technology services and products. Computer security consultants said the flaws could have had consequences ranging from corporate espionage to bid tampering. They also said the agency now faced the challenge of verifying the accuracy of contracting data. The site remained inoperative Friday morning, January 13, with a posted message stating: "The eOffer system is down for maintenance. Please pardon the inconvenience, thank you."
Source: http://www.nytimes.com/cnet/CNET_2100−1029_3−6026809.html

36. *January 13, FrSIRT* — **Toshiba Bluetooth stack file upload directory traversal vulnerability.** A vulnerability has been identified in Toshiba Bluetooth Stack, which could be exploited by remote attackers to place malicious files to arbitrary locations. Analysis: This is due to an input validation error in the OBEX Push services when processing uploaded files containing specially crafted file names, which could be exploited by attackers to upload malicious files to specific locations on an affected system by convincing a user to accept a connection request. The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/0184

37. *January 13, Tech Web* — **Million Dollar Homepage targeted in huge denial of service attack.** The Million Dollar Homepage, an ad gimmick created by British college student Alex Tew that brought more than $1 million to its 21−year−old creator, was under a massive denial of service attack Friday, January 13, the Website's hosting company said. Tens of thousands of computers controlled by an unknown group or person overwhelmed the site's servers with requests. The site was up Friday due to the voluntary efforts of the hosting company, InfoRelay Online Systems Inc. Tew drew international attention when his September idea to sell a million pixels on his homepage for a $1 each to advertisers took off. The attack stemmed from a network of computers, called a botnet, that were infected with Trojans or other malicious

software distributed over the Internet, Russell Weiss, vice president of technical services for InfoRelay, said. The attack started Wednesday night, January 11, growing by early Thursday, January 12, into a zombie army of possibly as many as 100,000 computers from all over the world, Weiss said. Weiss did not know where the attack originated, or whether it was part of an extortion scheme.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/13/AR2006011300210.html

38. *January 12, FrSIRT* — **Cisco Aironet Wireless Access Points denial of service vulnerability.** A vulnerability has been identified in Cisco Aironet Wireless Access Points (AP) running IOS, which may be exploited by remote attackers to cause a denial of service. This flaw is due to an error in the management interface that does not properly handle spoofed ARP (Address Resolution Protocol) messages, which could be exploited by an attacker who has successfully associated with a vulnerable device to exhaust all available memory resources and cause a denial of service. Solution: Upgrade to Cisco IOS version 12.3−7−JA2: http://www.cisco.com/public/sw−center/sw−wireless.shtml.
Source: http://www.frsirt.com/english/advisories/2006/0176

39. *January 12, Internet News* — **IBM, Sony, Toshiba build on cell deal.** IBM, Sony and Toshiba are renewing their joint chip development, extending it with a new, five−year term. The companies said the extension will enable them to work on 32 nanometer related research and advanced process technologies. "By extending this relationship to the next−generation of process technologies and deepening our partnership at the research level, we expect to increase the pace of development for major technology advances," said Lisa Su, vice president of semiconductor research and development at IBM. Sony's, IBM's and Toshiba's roots are deep. Since 2001, the partners have collaborated on 90 and 65 nanometer based process technologies, including the "Cell" microprocessor, which became available last February.
Source: http://www.internetnews.com/dev−news/article.php/3577136

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 an active malicious website that exploits a vulnerability in the Sun Java JRE. The initial report led US−CERT to believe the website was exploiting VU#974188. After further analysis, it was determined that the actual vulnerability being exploited was VU#760344. This vulnerability allows a Java Applet to bypass java security settings. Once these checks are bypassed, a remote attacker may be able to exploit this vulnerability to execute arbitrary code on the host machine.

More information about these vulnerabilities can be found in the following

US−CERT Vulnerability Notes:

VU#760344 Sun Java Plug−in fails to restrict access to private Java packages: http://www.kb.cert.org/vuls/id/760344

VU#974188 Sun Java Runtime Environment "reflection" API privilege elevation vulnerabilities: http://www.kb.cert.org/vuls/id/974188

US−CERT strongly encourages users and administrators to review the following mitigation to address this vulnerability as soon as possible:

Upgrade to the latest JRE

Do not access Java Applets from untrusted sources

Disable Java support in web browsers

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 34285 (−−−), 6881 (bittorrent), 445 (microsoft−ds), 25 (smtp), 27015 (halflife), 139 (netbios−ssn), 135 (epmap), 80 (www), 113 (auth) 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

40. *January 14, Associated Press* — **Engineers race to fix New Orleans levees.** In New Orleans, the apocalyptic clock is ticking −− again. Ravaged last year by one hurricane and slapped by the fringes of another, the city faces a 2006 storm season that begins in less than five months −− not much time to repair the tattered ramparts that keep New Orleans from being swallowed by the sea. This year's hurricane season begins June 1. By that date, the U.S. Corps of Engineers expects to have the Crescent City's levees restored to pre−Katrina condition. The job is massive. It will take about four million cubic yards of fill −− a nearly Superdome−sized pile −− to repair the 170 miles of levee destroyed or damaged by Katrina. Ivor van Heerden, a civil engineer at Louisiana State University, said, "We really need to go the step further and start implementing projects now that would make New Orleans safe." Col. Lewis Setliff, the leader of the repair effort, says as commander of Task Force Guardian, his mission is to repair the levees in time for the next hurricane season, and that is what he vows to do. New Orleans will simply have to live through 2006 with roughly the same protection it has had for the past 30 years.
Source: http://www.newsday.com/news/nationworld/nation/ats−ap_us11jan14,0,3565740.story?coll=ny−leadnationalnews−headlines

41. *January 14, United Press International* — **New York officials concerned over Gilboa Dam.** New York officials are watching the Gilboa Dam, built in 1926 to supply water to New York City, because it doesn't meet inspection standards. Routine inspections last October indicated the 182−foot−tall structure no longer met safety requirements, and emergency repairs are being made. If disaster struck the dam, all 19 billion gallons of the Schoharie Reservoir would cause massive flooding for miles, including the villages of Schoharie and Middleburgh, which could fill with 30 feet of water or more.
Source: http://www.sciencedaily.com/upi/?feed=TopNews&article=UPI−1−20060115−00053600−bc−us−dam.xml

[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