# Department of Homeland Security Daily Open Source Infrastructure Report for 11 January 2006

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

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

**Daily Highlights**

- The Federal Energy Regulatory Commission has directed PJM Interconnection and Potomac Electric Power Co. to develop a comprehensive plan to preserve regional reliability throughout the Washington, DC area. (See item 4)
- The Associated Press reports the Transportation Security Administration says the busiest U.S. airports −− about 40 of them −− will have bomb−detection equipment known as "puffer machines" installed by spring. (See item 17)
- The Associated Press reports police defused an explosive device found in the bathroom of a San Francisco Starbucks on Monday, January 9. (See item 36)

**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 10, Washington Post* — **Cnooc buys oil interest in Nigeria; seeks partnerships with rogue countries.** The Chinese state−controlled energy company Cnooc Ltd. has announced a $2.27 billion deal to buy a 45 percent stake in an offshore oil field in Nigeria, its first major foreign foray since its failed effort to purchase the American firm Unocal Corp. last summer. China imports about 40 percent of its crude oil, with more than half coming from the Middle

East. But growing concern about instability in the region −− a fact underscored by the U.S.−led war in Iraq, once a centerpiece of China's oil aims −− has prompted Beijing to seek sources elsewhere. In its quest for energy, China has shown a willingness to do business with regimes shunned as pariahs by much of the rest of the world for human rights abuses. Beijing once signed an energy deal with Iran at a time when the United States and Europe were debating whether and how to sanction the country for pursuing a nuclear weapons program. The Nigeria deal should be easier than the torturous process triggered when it tried to buy Unocal last summer. At a time of mounting trade tensions between the United States and China, critics in Congress branded the venture a threat to U.S. national security.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01/09/AR2006010901779_pf.html

2. *January 10, Energy Information Administration* — **Short−Term Energy Outlook January 2007.** In 2006 and 2007, total domestic energy demand is projected to increase at an annual rate of about 1.4 percent each year, contributing to continued market tightness and projected high prices for oil and natural gas. Prices for crude oil, petroleum products, and natural gas are projected to remain high through 2006 before starting to weaken in 2007. For example, the price of West Texas Intermediate crude oil, which averaged $56 per barrel in 2005, is projected to average $63 per barrel in 2006 and $60 in 2007. Retail regular gasoline prices, which averaged $2.27 per gallon in 2005, are projected to average $2.41 in 2006 and $2.33 in 2007. Henry Hub natural gas prices, which averaged $9.00 per thousand cubic feet in 2005, are projected to average $9.80 in 2006 and $8.84 in 2007.
Source: http://www.eia.doe.gov/steo

3. *January 09, News.com (Australia)* — **Australian gas set for U.S. sale.** White House officials are working to clear the final barriers to the sale of billions of dollars worth of Australian gas to the U.S. by the end of the decade. Speaking ahead of talks in Sydney, Australia, this week on energy markets, the U.S. Government expressed interest in seeing Australian liquefied natural gas (LNG) gain direct access to U.S. customers for the first time. Approval for a gas terminal −− which would be located offshore from Oxnard, north of Los Angeles −− could have shipments of Australian LNG sent to the U.S. market by the end of the decade. James Connaughton, President Bush's adviser on the environment, says: "Having LNG as an opportunity in the U.S. enhances our energy security because it promotes a diversity of potential future supply so we're not reliant on one particular area...We have a dedicated commitment to opening up the opportunity for a lot more LNG to America." Since the mid−1990s, imports of LNG to the U.S. have been rising fast. Annually, the U.S. consumes the equivalent of all the gas reserves off the western coast of Australia and growth in energy consumption may exceed 1.5 percent a year.
Source: http://www.news.com.au/story/0,10117,17763671−2,00.html?from =rss

4. *January 09, Federal Energy Regulatory Commission* — **Pepco, PJM directed to develop comprehensive plan to assure continued power grid reliability.** The Federal Energy Regulatory Commission (FERC) −− finding that reliability standards are not being met during certain conditions, and that the long−term reliability of the regional power grid in the Washington, DC, area is compromised −− directed the PJM Interconnection (PJM) and Potomac Electric Power Co. (Pepco) to develop a comprehensive plan to preserve regional reliability. The action complements an emergency order issued by Energy Secretary Samuel W.

Bodman last month requiring the Mirant Potomac River Generating Station to operate as needed to meet demand if key transmission lines serving Washington, DC, are out of service. Within one month of the order, PJM and Pepco are to file a comprehensive plan for the "operation, planning and construction of transmission facilities to address the current reliability risks to the system." The Commission noted that the Department of Energy emergency order "has not required the transmission entities to operate in accordance with applicable reliability standards or to identify the necessary operational, planning, and construction milestones necessary to address the reliability risk." Acting for the first time under section 207 of the Federal Power Act, the order responds to a complaint filed about reliability concerns regarding Mirant's cessation of operations at an Alexandria, VA, plant.
Source: http://www.ferc.gov/press−room/press−releases/2006/2006−1/01 −09−06−pepco.asp

5. *January 09, U.S. Nuclear Regulatory Commission* — **Nuclear Regulatory Commission finalizes "white" finding for Oyster Creek Nuclear Plant over classification of emergency.** The Oyster Creek nuclear power plant in Lacey Township, NJ, will receive additional oversight from the Nuclear Regulatory Commission (NRC) based on an inspection finding involving the classification of an emergency. The finding, which has now been finalized, stems from a failure by plant operators to properly use the plant's emergency action level matrix during an event in August. A "white" safety issue of low to moderate safety significance was declared. Because this was the second "white" inspection finding in the Emergency Preparedness cornerstone for the plant during the last year, Oyster Creek moved from the Regulatory Response Column to the Degraded Cornerstone Column of the NRC's Action Matrix, resulting in a higher level of scrutiny in the emergency preparedness area. NRC Region I Administrator Samuel J. Collins wrote to AmerGen, "Had the event degraded further, state and local agencies, who rely on information provided by the facility licensee, might not have been able to take initial offsite response measures in as timely a manner." AmerGen's corrective actions include enhanced training for control room operators and emergency response organization personnel, the assignment of a full−time human performance manager for operations, and staffing improvements throughout the site.
Matrix: http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/actionmatrix_summary .html.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2006/06−0 02i.html

6. *January 08, Scotland on Sunday (UK)* — **Oil imports fuel looming energy crisis.** The International Energy Agency (IEA) has warned that the UK economy will become a net importer of oil this year for the first time in more than a decade −− three years earlier than the government has predicted. IEA has forecast that North Sea oil production will dip below 1.7 m barrels per day this year, forcing the economy to rely on more imported supplies to meet demand. The warning follows the Russian decision to shut off gas to Europe that thrust energy security into the foreground and further emphasizes the extent of the British government's failure to anticipate energy threats to the economy. The International Energy Agency's supply analyst David Fyfe said, "Given expected oil production this year of below 1.7 m barrels per day, the UK faces the prospect of becoming a net crude importer again this year for the first time since 1992." The government's more optimistic forecasts, however, do not see the UK becoming a net importer until 2010. The news will also come as a shock to UK oil producers who share the government's optimistic forecast. Peter Spencer, chief economist for UK Item Club, said the shift would be mainly symbolic for the UK economy.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8

knpq%5F%5BfkppsqsZSmk%7D38%7Dbfel%5Dv

7. *January 06, NERC News* — **Report names entities confirmed to have violated North American Electric Reliability Council standards.** The North American Electric Reliability Council (NERC) has found 57 instances of noncompliance with NERC reliability standards and 54 instances of noncompliance with regional standards that occurred during the third quarter of 2005. Of these 111 instances of noncompliance, 42 have been confirmed. The Compliance Enforcement Program Report for the third quarter of 2005, which NERC posted in December, identifies those entities confirmed to have violated NERC or regional reliability standards during the third quarter. The report also lists, without identifying the entities involved, unconfirmed violations that are still undergoing review by appropriate authorities. To help assess the effect of a violation, each region supplies a reliability impact statement for violations within the region. These statements provide more information about the violations and how they may or may not affect the system. The Compliance and Certification Managers Committee conducts a peer review of the violations to promote consistency among the regions in determining the significance of the violations and the relative potential of the violations to cause widespread cascading outages on the bulk power system.
   Compliance report: http://www.nerc.com/~comply/quarterly.html.
   Source: http://www.nerc.com/~filez/nercnews/news−0106c.html

8. *January 06, Department of Homeland Security* — **Domestic Nuclear Detection Office to conduct nuclear detector systems testing in Nevada.** The Domestic Nuclear Detection Office (DNDO) announced that it will be testing current and prototype next−generation handheld and mobile nuclear detectors at the Nevada Test Site (NTS) from Monday, January 9, through Friday, February 3, 2006. The testing will subject detectors to a series of realistic materials and threats encountered in legitimate commerce, as well as occur in potentially illicit activities. DNDO will make the evaluations available to state and local agencies to aid their selection and acquisition of preventive nuclear detection equipment using Department of Homeland Security (DHS) grants. “A critical component of the Domestic Nuclear Detection Office’s program is high fidelity testing and evaluation, using test objects and configurations representative of actual threats,” said Vayl Oxford, the DNDO Director. DNDO was established in April 2005 to coordinate and improve the ability of the U.S. Government to counter the threat of terrorist nuclear attack. To date, DNDO and CBP have deployed over 650 portal monitors to the nation’s ports of entry. DNDO and the DHS Office of Grants and Training are working with representatives from 34 state and local agencies to develop comprehensive domestic nuclear detection programs, to include planning, exercises, training, and acquisition of detection systems.
   Source: http://www.dhs.gov/dhspublic/display?content=5333

[Return to top]

## Chemical Industry and Hazardous Materials Sector

9. *January 10, Los Angeles Times* — **Fiery blasts at California paint plant injure three, prompt business evacuations.** A fire and a series of explosions ripped through a paint manufacturing facility in Carson, CA, on Monday, January 9, critically injuring three people and forcing the evacuation of surrounding businesses. The fire erupted at Advanced Packaging

and Products in the 16000 block of Maple Avenue shortly after 12 p.m. PST, triggering blasts that shot flames, along with canisters and other debris, up to 70 feet in the air. A towering column of black smoke was visible for miles. The three male burn victims, who were not immediately identified, were taken to hospital burn units, officials said. Dozens of firefighters responded to the blaze, and about 100 employees from neighboring businesses in the industrial district were evacuated as a precaution. It took about 75 Los Angeles County and city firefighters about an hour to extinguish the blaze. The cause of the fire is under investigation. Records did not indicate any violations by the company in the past year. But the plant has been cited for serious violations in the past, according to the state Division of Occupational Safety and Health.
Source: http://www.latimes.com/news/local/la−me−fire10jan10,1,6802994.story?coll=la−headlines−california

[Return to top]

## Defense Industrial Base Sector

**10.** *January 03, Defense Link* — **New device will sense through concrete walls.** Troops conducting urban operations soon will have the capabilities of superheroes, being able to sense through 12 inches of concrete to determine if someone is inside a building. The new "Radar Scope" will give war fighters searching a building the ability to tell within seconds if someone is in the next room, said Edward Baranoski from the Defense Advanced Research Projects Agency's (DARPA) Special Projects Office. By simply holding the portable, handheld device up to a wall, users will be able to detect movements as small as breathing, he said. The Radar Scope, developed by DARPA, is expected to be fielded to troops in Iraq as soon as this spring, Baranoski said. Even as the organization hurries to get the devices to combat forces, DARPA already is laying groundwork for bigger plans that build on this technology. Proposals were given last week for the new "Visi Building" technology that's more than a motion detector. It will actually "see" through multiple walls. The device is expected to take several years to develop. Ultimately, service members will be able to use it simply by driving or flying by the structure under surveillance, Baranoski said.
Source: http://www.defenselink.mil/news/Jan2006/20060103_3822.html

[Return to top]

## Banking and Finance Sector

**11.** *January 10, BusinessWeek* — **The booming business of ID protection.** Consumers and small−business managers are being offered a growing number of financial products aimed at safeguarding against ID theft −− a crime that, according to Javelin Strategy & Research, affected about 9.3 million people in 2004, causing $52.6 billion in losses in the U.S. alone. On average, ID−theft victims rack up $500 in costs and take 30 hours to solve a case, according to the U.S. Federal Trade Commission. "The whole ID−theft insurance industry has developed significantly in the last two years," says Beth Givens, director of the Privacy Rights Clearinghouse, a San Diego−based consumer−advocacy group. In a 2005 Javelin survey of 2,200 consumers, 34 percent of respondents chose identity−fraud insurance as one of three

additional security measures they would most like financial−services companies to provide, and 45 percent prioritized a full guarantee against identity fraud. American International Group says it covers about seven million people against ID theft, compared with about five million a year ago. St. The number of people victimized by ID theft amounts to about four percent of the 215 million adults who have active credit tracked by credit−scoring company Experian.
Source: http://www.businessweek.com/technology/content/jan2006/tc200 60110_146542.htm

12. *January 09, Navy NewsStand* — **Scam artists directed to Navy Web portal.** The Naval Education and Training Command (NETC) at Naval Air Station (NAS) Pensacola, FL, is warning users of the Navy Knowledge Online (NKO) Web portal to be alert for an Internet phishing scam that is being directed at users of NKO. NETC officials are issuing an alert to inform NKO users of their potential vulnerability to this scheme. The NKO scam was first identified in early December, in an attempt to exploit “multiple vulnerabilities” in Microsoft’s Internet Explorer Web browser. Victims received e−mails appearing to be from NKO informing them to visit the NKO Web portal to reset their passwords. Upon receipt of the e−mail and selecting the embedded link, users are redirected to a false site that resembles the NKO front page and are directed to login using their current password and submit a new password. Once users have logged in to the fake site, an executable data file is activated. Navy officials have identified this file as a “JavaScript vulnerability.” Peg David, NKO program manager, said “Military and civilian computer users should know that NKO, the Navy and most reputable businesses do not contact their customers and request them to divulge personal information or passwords in this manner."
Source: http://www.news.navy.mil/search/display.asp?story_id=21601

13. *January 09, The Guardian (UK)* — **ID theft risk elevated as thousands of credit card slips found dumped in UK dumpster.** Thousands of documents revealing the credit card numbers, addresses, phone numbers and signatures of guests were dumped in an open dumpster by one of Britain's best−known hotels in what one fraud expert described as "the biggest field day for identity [scammers] we have seen". Staff threw out registration forms and credit card slips of guests who stayed at the hotel between 1998 and 2000. Each one listed the name, company, home address and credit card number in full. Most included a home phone number, and in the case of some foreign guests, passport numbers. One of the UK's leading experts on ID fraud, Professor Martin Gill of the University of Leicester, described the hotel's actions as "incredibly negligent," and said "This could be the biggest thing of this type to hit business in the UK." Half the documents were not in sealed envelopes, and the UK's Data Protection Act requires all documents to be disposed of securely, preferably by shredding.
Source: http://travel.guardian.co.uk/news/story/0,7445,1682378,00.ht ml

14. *January 09, eWeek* — **More time being spent by IT managers on data theft protection.** Chief Information Officers (CIOs) are spending more time on varied ways to protect against data theft. Thaddeus Arroyo, Cingular's CIO, provides resources for data backups and recovery, to hedge against the possibility that hackers will attack Cingular's network. Richard Reeder, CIO of the State University of New York's Stony Brook campus, said he worries about credit card information of students who pay for courses online, illegal downloads, and system upgrades. Security and IT risk management, rather than system maintenance, consumes at least 10 percent of his attention every day, Reeder estimated. At Arch Chemicals Inc., Vice President of IT Al Schmidt said he has −− using a risk−assessment methodology developed by the

Government Accounting Office −− developed a "threat library" for the $1.4 billion chemical wholesaler. He documented risks along Arch's supply chain and then played out various risk scenarios to gauge their severity. Arroyo, at Cingular, puts specific numbers on the possible damage from an IT risk −− for example, the lost revenue from a virus knocking Cingular's subscribers off the network for an hour. Where a threat does not lend itself to financial measurement, Arroyo describes potential damage as "small," "medium" or "large," a qualitative risk assessment.
Source: http://www.eweek.com/print_article2/0,1217,a=168398,00.asp

[Return to top]

## Transportation and Border Security Sector

**15.** *January 10, USA TODAY* — **Airlines change how they get people aboard.** Industry giants United Airlines and Delta Air Lines, as well as discounter AirTran, have abandoned the traditional back−to−front boarding of their coach sections. America West has made the move, too. The motive: Time is money for airlines trying to stick to a schedule and to keep their planes flying as many hours as possible. Traditional back−to−front boarding clogs the cabin by drawing too many people into a confined area at once, says Eitan Bachmat, a professor of Israel's Ben Gurion University of the Negev. One example: United now groups passengers at the gate according to their seat's letter designation. The carrier boards window passengers first, followed by those in middle and aisle seats. Its boarding is now four to five minutes faster, saving the company about $1 million a year, says spokesperson Robin Urbanski. AirTran's new procedure, introduced last July, boards passengers in the back four rows first, followed by the front four rows. The process is repeated until the cabin is full. Delta Air Lines uses a variation in its new system, introduced in early 2004: The zone that includes the back few rows boards first, then a middle section followed by a front section. It then goes back to a rear section.
Source: http://www.usatoday.com/travel/news/2006−01−09−boarding−usat_x.htm

**16.** *January 10, Department of Transportation* — **Federal Highway Administration provides money to help California reduce congestion.** The Federal Highway Administration (FHWA) on Tuesday, January 10, provided more than $3 million in federal grant funds to help California explore new ways to reduce congestion through projects like high−occupancy toll (HOT) toll lanes. The grants are part of the FHWA Value Pricing Pilot Program to fund testing and evaluation of innovative ways to reduce traffic congestion. The landmark highway, transit and safety legislation signed in August by President Bush gives states more flexibility to use tolling, HOT lanes and other congestion solutions to offer drivers more choices for a reliable trip. With HOT lanes, low−occupancy vehicles are charged a toll while high−occupancy vehicles may use the lane at no charge or at a discounted rate. “The Bush Administration championed tolling in the new transportation law so states would have more innovative ways to tackle congestion and give drivers more choices to get home or to work,” said Acting Federal Highway Administrator J. Richard Capka. In addition to keeping lanes free flowing, tolling generates revenue for transportation improvements and expansion, according to Capka.
The Value Pricing Pilot Program Grants table: http://www.dot.gov/affairs/vppgrants.htm
Source: http://www.dot.gov/affairs/fhwa0106c.htm

**17.**

*January 10, Associated Press* — **Dallas/Fort Worth among 40 airports to get bomb−detection devices.** The busiest U.S. airports −− about 40 of them, including Dallas/Fort Worth International −− will have bomb−detection equipment known as "puffer machines" installed by spring, the Transportation Security Administration said Monday, January 9. There are now 24 airports with the walkthrough machines, which puff air onto a person to dislodge tiny particles from skin and clothing. The machine sucks up the particles and then analyzes them for traces of explosives. One of the biggest weaknesses in U.S. airport security has been the limited ability to detect bombs on passengers. Government screeners have relied largely on patdowns, which are unpopular, time−consuming and incomplete. In contrast, a puffer machine takes 17 seconds to check a passenger and can analyze particles as small as one−billionth of a gram. "It's more comprehensive and more accurate, and it limits the number of patdowns," said TSA spokesperson Darrin Kayser. Four of the machines were installed at D/FW in July, coinciding with the opening of Terminal D, the airport's new international facility. Three of the phone−booth size devices are in Terminal D, the fourth is in Terminal C. The airport has requested 15.
Source: http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/011006dnnattsa.d09129d.html

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

18. *January 10, Agricultural Research Service* — **New approaches needed to fight cattle virus.** Agricultural Research Service (ARS) scientists are ready to take to the next level efforts to eradicate the bovine viral diarrhea virus (BVDV). BVDV causes animal diseases that affect reproduction and nutrition, milk production, and respiratory function. Pregnant cows that are infected can have spontaneous abortions or give birth prematurely, while calves born with BVDV may be persistent carriers that can infect additional herds. There's no treatment for BVDV, which costs U.S. cattle producers millions of dollars in losses each year. According to ARS microbiologist Julia Ridpath, decades of vaccination and voluntary control programs aimed at eliminating the virus from the U.S. have not worked. An extensive management program encompassing vigilance, biosecurity education, and continued research is needed. She recently launched a study with the Northeast Iowa Dairy Foundation focusing on newborn calves' response to BVDV vaccination. ARS microbiologist John Neill is applying serial analysis of gene expression (SAGE) −− a technology developed for detecting gene−expression alterations that tell how cancer cells differ from normal cells −− against BVDV. Neill is using SAGE to compare cattle gene expression in normal cells to that in BVDV−infected cells. He's also studying the pathology and immunosuppressive properties of the virus.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

19. *January 10, Animal and Plant Health Inspection Service* — **U.S. Department of Agriculture**

**tree climbers continue to search for invasive beetle.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service, Asian longhorned beetle (ALB) cooperative eradication program, will begin climbing surveys of 1,800 trees in the northwest section of Linden, NJ, to search for signs of the invasive pest. Starting January 3, and lasting until early March, climbers will examine hard−to−reach areas of 1,800 residential and street trees. Trained personnel will search high in tree limbs and among tree canopy branches for the tell−tale signs of beetle activity such as the circular, dime−sized holes made by mature beetles upon exiting trees, and egg sites that indicate the invasive pest is likely spending the winter maturing deep within a tree's heartwood. The tree−killing beetles were discovered in the Middlesex/Union County area in 2004. Shortly after their discovery, the area was quarantined to curtail the movement of wood, wood products, and debris that could contain beetles in various developmental stages. The ALB, which likely hitchhiked to the U.S. from Asia within solid wood packing material, is a serious threat to the nation's hardwood trees. This beetle has the potential to damage such industries as lumber, maple syrup, and nursery, accumulating over $41 billion in losses.
Source: http://www.aphis.usda.gov/newsroom/content/2006/01/nj_alb.sh tml

**20.** *December 12, American Farm Bureau Federation* — **Farm Bureau study identifies agriculture's future challenges.** Over the next 15 years, American agriculture will remain a productive and profitable venture, but the industry will look considerably different than it does today. According to a two−year Farm Bureau study, U.S. agriculture's future will include a drastically changed government farm program, continued consolidation of production, and the adoption of additional environmental practices dictated by the marketplace. The study was conducted by the Making American Agriculture Productive and Profitable (MAAPP) Committee. The MAAPP committee consisted of 23 Farm Bureau farmers and ranchers from across the nation that spent two years studying the possible structure of U.S. agriculture in the year 2019. The committee identified various trends and circumstances affecting the future of farmers and ranchers. Perhaps one of the most glaring areas in the report deals with the future structure of American agriculture. In 2002, 143,000 farming operations produced 75 percent of the value of all agricultural output. It took 1.9 million operations to produce the remaining 25 percent. According to the report, however, by 2019, there will be more large farms and more small farms, but the number of mid−sized farms will have decreased drastically. The report also explored the relationship between farmers and their rural communities.
Source: http://www.fb.org/news/nr/nr2005/nr1212c.html

[Return to top]

## Food Sector

**21.** *January 09, Food and Drug Administration* — **Smoked trout recalled.** Whole Foods Market is recalling Whole Catch Lemon Pepper Garlic Hot Smoked Trout because it has the potential to be contaminated with Listeria monocytogenes, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. The product, distributed by Whole Foods Market, may have reached consumers via stores in the following states: California, Florida, Kentucky, Massachusetts, Maryland, New Jersey, New York, North Carolina, Pennsylvania, Virginia, and the District of Columbia. No illnesses have been reported to date. The recall was initiated after random testing

by the Florida Department of Agriculture and Consumer Services, Division of Food Safety. Other batches and other varieties of this product are not affected by this voluntary recall. The company continues an investigation as to what may have caused the problem.
Source: http://www.fda.gov/oc/po/firmrecalls/wholefoods01_06.html

[Return to top]

## Water Sector

Nothing to report.
[Return to top]

## Public Health Sector

**22.** *January 10, Reuters* — **Turkey battles to contain bird flu outbreak.** Turkey reported another case of bird flu in a patient in the center of the country on Tuesday, January 10, as the authorities sealed off parts of the outskirts of major cities Ankara and Istanbul while they culled poultry. Three children have already died in eastern Turkey −− the first reported deaths from the bird virus flu outside China and Southeast Asia. Four people were taken to hospital with suspected bird flu in the town of Aydin near the Aegean coast. Turkey has now confirmed 15 people with bird flu infections since last week, most in eastern, central, and northern parts of the country. More than 70 people are suspected of having the bird flu virus and are undergoing tests. Health experts say the outbreak in Turkey is the worst since one in Hong Kong in 1997 when 18 people were infected and six died before it was brought under control. Bird flu has killed at least 76 people since it reemerged in late 2003. Parts of the capital Ankara and the business hub Istanbul have been sealed off for the culling of poultry. Inhabitants leaving the areas have been disinfected.
Source: http://today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2006−01−10T103423Z_01_DIT955429_RTRUKOC_0_US−BIRDFLU−TURKEY.xml&archived=False

**23.** *January 10, Agence France−Presse* — **Japan says 77 infected in past with mild bird flu.** Seventy−seven poultry workers in Japan have tested positive for bird flu in the first−ever human infections involving the weaker strain of the virus that has hit its chicken industry, the government said. The farm workers in Ibaraki and Saitama prefectures, both north of Tokyo, were infected at some point in the past but currently show no symptoms, the health and welfare ministry said Tuesday, January 10. The ministry said the workers posed no risk to others and had the H5N2 virus, a milder strain than H5N1 which has killed more than 75 people since 2003. "The result of the tests showed that a total of 77 people were carrying antibodies supposed to be created following an infection of H5N2," a ministry official said. "It was the first ever case in the world showing a human infection of H5N2," the official said, adding however that developing countries hit hardest by bird flu rarely bother trying to confirm cases of the weaker strain. The ministry and the National Institute of Infectious Diseases carried out tests on 350 workers and their families at affected chicken farms.
Source: http://news.yahoo.com/s/afp/20060110/hl_afp/healthflujapan_060110124151;_ylt=AheEH6IQpcCXQNhloJrsxGWJOrgF;_ylu=X3oDMTBiM

W04NW9mBHNlYwMlJVRPUCUl

**24.** *January 10, USA Today* — **States average a C−minus for emergency care.** Emergency medical care in the U.S. rates a C−minus, with hospitals increasingly facing overcrowding, a lack of financial support, and a growing number of uninsured patients, a physicians' group warns. In the first national assessment of its kind, the American College of Emergency Physicians used data from government and private sources to rate states on 50 measures, ranging from access to emergency care to state policy issues, such as laws requiring seat belt use, and the amount spent training emergency workers. The American College of Emergency Physicians used 50 criteria to determine the quality of emergency care in each state. They graded such things as access to care, state financing and policies around injury prevention. The nation as a whole received a grade of C−, the average of all state grades. No state got an A. Nationwide, problems include overcrowded or understaffed hospitals. Ambulances are sometimes diverted away from such facilities to hospitals further away. Quality of care, physician training and whether states cap non−economic damages in medical malpractice lawsuits were also among the measures.
National report: http://my.acep.org/site/DocServer/2006−NationalReportCard.pd f?docID=221
Source: http://www.usatoday.com/money/industries/health/2006−01−10−e mergency−usat_x.htm

**25.** *January 10, Itar−Tass (Russia)* — **Russia tightens control over health of arrivals from Turkey.** Russia's chief sanitary doctor Gennady Onishchenko was ordered to tighten control on the border over the health of the people arriving from Turkey and neighboring countries. "Due to the epizooty of flu among domestic and wild foul in Turkey, and the registered occurrence of fatal cases of bird flu among people, the Federal Service for Consumer Rights and Human Welfare asks to tighten control over the health of people arriving from Turkey and neighboring countries at the checkpoints on the state border," Onishchenko said in a letter sent to the chief sanitary doctors of the republics of North Ossetia and Dagestan.
Source: http://www.itar−tass.com/eng/level2.html?NewsID=2779239&Page Num=0

**26.** *January 09, Associated Press* — **Nursing shortage expected to quintuple by 2020.** Like many other states, Maine has a nursing shortage. The Maine Department of Labor reported nearly 1,100 annual nursing vacancies statewide, and the shortfall is expected to grow to more than 5,200 by 2020. A bill before the Maine Legislature attempts to address the nursing shortage. It seeks $1.7 million more for nursing programs across the state in an effort to increase nursing student slots.
Source: http://www.wmtw.com/news/5945136/detail.html?rss=port&psp=ne ws

**27.** *January 09, Arizona State University* — **Plant−derived vaccines safeguard against plague.** Researchers in the Biodesign Institute at Arizona State University have successfully turned tobacco plants into vaccine production factories to combat the deadliest form of plague. The vaccine elicits a protective immune response in guinea pigs. Plague is caused by a rod−shaped bacterium called Yersinia pestis. "There have been discovered some resistant strains to antibiotics and that poses a concern, especially if plague would be used as a bioweapon," said Luca Santi, lead author of the study. "A new vaccine approach would be the best way to prevent infection." Current vaccines against plague are severely limited from widespread adoption by having problems with high adverse reaction rates and side effects. The research

team worked out a new plant−based system to rapidly and stably produce high levels of proteins, called antigens, which conferred immunity against the plague. The researchers modified tobacco plants to make high levels of the plague antigens F1, V and a combination of the two, a so−called F1−V fusion antigen. All are known to be important for the plague bacteria to produce its toxic effects.
Source: http://www.biodesign.asu.edu/news/113/

28. *January 09, Archives of Internal Medicine* — **Population−based study from a rural area in Vietnam with outbreaks of highly pathogenic avian influenza.** The verified human cases of highly pathogenic avian influenza in Vietnam may represent only a selection of the most severely ill patients. The study objective was to analyze the association between flu−like illness, defined as cough and fever, and exposure to sick or dead poultry. A population−based study was performed from April 1 to June 30, 2004, in FilaBavi, a rural Vietnamese demographic surveillance site with confirmed outbreaks of highly pathogenic avian influenza among poultry. Researchers included 45,478 randomly selected (cluster sampling) inhabitants. Household representatives were asked screening questions about exposure to poultry and flu−like illness during the preceding months; individuals with a history of disease and/or exposure were interviewed in person. A total of 8,149 individuals (17.9 percent) reported flu−like illness, 38,373 persons (84.4 percent) lived in households keeping poultry, and 11,755 (25.9 percent) resided in households reporting sick or dead poultry. A dose−response relationship between poultry exposure and flu−like illness was noted. The flu−like illness attributed to direct contact with sick or dead poultry was estimated to be 650 to 750 cases. The epidemiological data are consistent with transmission of mild, highly pathogenic avian influenza to humans and suggest that transmission could be more common than anticipated, though close contact seems required.
Source: http://archinte.ama−assn.org/cgi/content/abstract/166/1/119

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

29. *January 09, South Florida Business Journal* — **Florida governor proposes hurricane readiness plan.** In response to consecutive years of devastating hurricanes, Florida Governor Jeb Bush, on Friday, January 6, disclosed a $565 million budget recommendation in state and federal funding designed to create what he called a "culture of preparedness." Some of the recommendations include about $300 million for affordable rental housing and ownership for the state's most vulnerable residents; nearly $70 million to expand county emergency operations centers; and $50 million to harden existing homes with the priority being given to low income homeowners. Bush noted that, "Government must prepare, but it is not the only solution…it's a civic responsibility for everyone in the state to be prepared." That means, in part, being ready before a storm strikes and being self−sufficient after a hurricane, he said, adding such actions

save lives, protect property and reduce costs. To raise awareness about the need to plan for such emergencies, the governor said he is proposing to spend $5.3 million on a public education and information campaign. He is also recommending last year's sales tax holiday for hurricanes supplies be made permanent and coincide with National Hurricane Preparedness Week in late May or just before the hurricane season begins.
Source: http://southflorida.bizjournals.com/southflorida/stories/200 6/01/09/daily11.html

30. *January 08, Reuters* — **China orders fast reporting of unrest, crises in new national emergency response plan.** Local Chinese officials must get news of unrest and other "emergencies" straight into the hands of central leaders to comply with new national emergency response measures, issued at the weekend. The plan divides natural disasters, public health and environmental crises and threats to social stability into four color−coded categories and sets different broad responses from local and central authorities to each. Local authorities must inform the State Council, China's cabinet, of "important social security incidents" within four hours, state the rules posted on the central government's Website. "The guidelines come at a time when a string of serious cases, including contamination of drinking water, bird flu outbreaks and mine accidents, have stricken China over the past few months," the China Daily said on Monday, January 2.
China Website: http://www.gov.cn.
Source: http://news.yahoo.com/s/nm/20060109/wl_nm/china_unrest_dc_1

31. *January 08, Associated Press* — **Singapore conducts drill to test readiness for terror attacks on transport system.** Singapore staged a large emergency exercise on Sunday, January 8, to test its readiness for terror attacks on its bus and subway systems, mindful that its role as a close U.S. ally makes it a potential target for Islamic extremists. More than 2,000 workers from 22 government agencies took part in the emergency exercise, which involved mock attacks at train stations and a bus interchange. Organizers used thunder flashes to simulate bomb explosions, as well as smoke generators, fire simulators and special makeup to simulate wounds. Hundreds of “casualties” wore tags detailing their simulated wounds −− including burns and injuries caused by chemical agents −− so paramedics knew how to “treat” them. Authorities had said they would hold the exercise on a weekend in the first half of January, but had not said exactly when. Service at a dozen train stations was disrupted for several hours, and shuttle bus service was provided for commuters. Public announcements were made just before the drill to avoid panic. Singapore, a strong backer of U.S. efforts to fight terror, is concerned about threats from Jemaah Islamiyah, a Southeast Asian terror group linked to al Qaeda.
Source: http://www.khaleejtimes.com/DisplayArticle.asp?xfile=data/theworld/2006/January/theworld_January151.xml&section=theworld &col

[Return to top]

## Information Technology and Telecommunications Sector

32. *January 09, Tech Web* — **More unpatched bugs loose in Microsoft Windows Metafile.** Just days after Microsoft rushed out a patch for a bug in Windows Metafile (WMF) image processing, a security company has warned customers that multiple memory corruption vulnerabilities in the same rendering engine could leave users open to attack. "An attacker may leverage these issues to carry out a denial of service attack or execute arbitrary code," Symantec

said in a vulnerability alert issued through its DeepSight Management System. The bugs may be associated with the one patched Thursday, January 5, by Microsoft, but they involve different functions of the Windows WMF rendering engine, added Symantec, which highlighted the various values and structures within the engine which could be exploited. "Reports indicate that these issues lead to a denial of service condition, however, it is conjectured that arbitrary code execution is possible as well," the Symantec alert went on. If true, the dangers of these new vulnerabilities are identical to the flaw that Microsoft fixed last week. Like that bug, these newly−discovered vulnerabilities can be exploited with a maliciously−crafted WMF file that's posted on a Website, opened from an e−mail attachment, or launched with Microsoft or third−party image applications.
Source: http://www.securitypipeline.com/news/175802826

**33.** *January 09, VNUNet* — **Sober worm infection rates are plummeting.** The Sober worm, which was due to activate last Thursday, January 5, has stopped spreading and its author has held back from uploading malware onto any machines. Sober was the most common infection in November and December last year, and was programmed to download software from remote Websites. It was feared that host machines across the world would start sending spam or take part in denial of service attacks. Instead the virus writer has stayed undercover and the worm has ceased trying to spread itself. "When the Sober.Y download deadline passed on 6 January all infected machines started download attempts from the five different sites. At the same time, the virus stopped e−mailing itself around," said Mikko Hyppönen, chief research officer at security firm F−Secure. "As a result, the virus that had held the number one position since November 2005 just disappeared from the stats." Hyppönen added that infection rates for the worm over the past week were running at 18,000 PCs per day but are now plummeting.
Source: http://www.vnunet.com/vnunet/news/2148257/quiet−sober−front

**34.** *January 09, CNET News* — **Microsoft to hunt for new species of Windows bug.** Microsoft plans to scour its code to look for flaws similar to a recent serious Windows bug and to update its development practices to prevent similar problems in future products. The critical flaw, in the way Windows Meta File (WMF) images are handled, is different than any security vulnerability the software maker has dealt with in the past, said Kevin Kean and Debby Fry Wilson, directors in Microsoft's Security Response Center. Typical flaws are unforeseen gaps in programs that hackers can take advantage of and run code. By contrast, the WMF problem lies in a software feature being used in an unintended way. In response to the new threat, the software company is pledging to take a look at its programs, old and new, to avoid similar side effects. Microsoft has been working for years to improve its security posture, beginning with its Trustworthy Computing Initiative, launched in early 2002. The WMF problem is not a good advertisement for Microsoft's security efforts, one analyst said, as the legacy issue seemingly went undetected. "This should have been caught and eliminated years ago," said Gartner analyst Neil MacDonald.
Source: http://news.com.com/Microsoft+to+hunt+for+new+species+of+Windows+bug/2100−1002_3−6024778.html?tag=cd.lede

**35.** *January 09, CNET News* — **Sprint Nextel suffers service outage.** Thousands of customers of Sprint Nextel wireless and its resellers, such as Virgin Mobile, were without service Monday, January 9, after the network suffered two separate fiber cuts, a company spokesperson said. At about 12:30 p.m. PST, a fiber cut between Palm Springs, CA, and Phoenix, AZ, had interrupted

service for Sprint Nextel's wireless, wireline and long−distance customers. Most of the customers affected were on the West Coast. But there were reports of service interruptions in the Midwest and on the East Coast, too. Sprint Nextel, like all major carriers, has a redundant fiber optic network, so if one link fails, traffic will be routed to another fiber without service interruption. But Monday, much of the traffic running on the Phoenix/Palm Springs link already had been rerouted from a link outside Reno, NV. Heavy rains in the area had caused what technicians refer to as a "washout." To repair the fiber, the company had to cut it and shift traffic from Reno to the Phoenix link while they repaired the fiber. These dual fiber cuts have resulted in dropped calls and outages of traffic going to and coming from western areas of the U.S., the company said in a statement.
Source: http://news.com.com/Sprint+Nextel+suffers+service+outage/2100−1037_3−6024922.html?tag=cd.top

## Internet Alert Dashboard

**DHS/US−CERT Watch Synopsis**

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

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

Opening a specially crafted WMF file which may be masquerading as a MS Word or MS Office document.

Opening a specially crafted WMF file which may be masquerading as a JPEG or other type of image file.

Visiting a specially crafted web site.

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

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

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

Execute arbitrary code

Cause a denial of service condition

Take complete control of a vulnerable system

More information about this vulnerability can be found in the following:

US−CERT Vulnerability Note: VU#181038 − Microsoft Windows Metafile handler SETABORTPROC GDI Escape vulnerability http://www.kb.cert.org/vuls/id/181038

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

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

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

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (win−rpc), 445 (microsoft−ds), 25 (smtp), 6881 (bittorrent), 139 (netbios−ssn), 27015 (halflife), 7008 (afs3−update), 135 (epmap), 80 (www), 6346 (gnutella−svc)<br>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

**36.** *January 10, Associated Press* — **Explosive device found at San Francisco Starbucks.** Police defused an explosive device found in the bathroom of a San Francisco Starbucks on Monday, January 9. No one was injured. Authorities were called around 1:15 p.m. PST, after an employee reported finding something suspicious in the store's bathroom. About 100 people were evacuated from the store and apartments above it, and the street was closed to traffic, said Sgt. Neville Gittens. "If it had exploded, it would have caused injuries or damage," said Gittens. Once the device was disabled at about 2:10 p.m., police allowed people back into the apartment building and reopened the street. Seattle−based Starbucks declined to provide further details. Source: http://www.usatoday.com/news/nation/2006−01−09−starbucks−exp losive_x.htm

[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