# Department of Homeland Security Daily Open Source Infrastructure Report for 26 January 2006

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

## Daily Highlights

- The Sun−Sentinel reports the Florida Public Service Commission is seeking ways to protect the electrical system from hurricanes, including make it easier to put lines underground; make it easier for power companies to trim trees; install stronger poles; and protect substations against flying debris. (See item 3)
- The Star−Ledger reports a temporary airport−like security system to detect explosives will be set up next month at the Exchange Place PATH station in Jersey City, as the first phase of a federal test program designed to increase rail safety across the country. (See item 14)
- The Columbus Dispatch reports the Ohio Retail Food Defense Preparedness Guide, available as a CD−ROM, provides detailed information to help grocers assess and address any vulnerability in the food supply from the delivery of the products to the retail stores, to the time they leave the store with the customer. (See item 23)



# 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 26, Utility Automation & Engineering* — **U.S. wind industry ends most productive year.** The U.S. wind energy industry easily broke earlier annual installed capacity records in

2005, installing nearly 2,500 megawatts (MW) or over $3 billion worth of new generating equipment in 22 states, according to the American Wind Energy Association (AWEA). Instead of the slow year that has previously followed boom years for the industry, 2006 is expected to be even bigger, with installations topping 3,000 MW, says the AWEA. The final tally of 2,431 MW boosted the cumulative U.S. installed wind power fleet by over 35 percent, bringing the industry's total generating capacity to 9,149 MW. The previous record capacity figure was set in 2001. There are now commercial wind turbine installations in 30 states. The growth in wind power construction comes at a time of electricity and natural gas rate hikes due to the natural gas supply shortage. AWEA estimates that an installed capacity of 9,149 MW of wind power will save over half a billion cubic feet of natural gas per day in 2006, alleviating a portion of the supply pressure. The U.S. currently burns about 13 Bcf/day for electricity generation, which means during 2006, wind power will reduce natural gas use for power generation by approximately five percent.
Source: http://uaelp.pennnet.com/Articles/Article_Display.cfm?ARTICL E_ID=246415&p=22

2. *January 24, Gannett* — **Scare causes nuclear plant lockdown.** The Davis−Besse Nuclear Power Station was locked down for three hours Monday, January 23, after a contractor falsely reported being carjacked while he was driving to the plant, officials said. When the contractor, John Edward Grochowski, arrived at the plant at 6:07 a.m. EST for his first day of work, he told a security officer three people jumped into his car after he saw a girl along the road and pulled over, according to the Ottawa County Sheriff's Office. The men held him at gunpoint, tried to tie a rope around his neck, and stayed in the car until he arrived at Davis−Besse, he told deputies. They fled when Grochowski stopped at the initial vehicle−security check, he told deputies. Thirty−two law enforcement officials combed the area around Davis−Besse for the men until Grochowski admitted at 9:45 a.m. EST he made up the story, Sheriff's Detective Joe Vidal said. The plant was taken out of lock down shortly after. Sheriff Bob Bratton said Grochowski gave no explanation for why he fabricated the attack. First Energy has used Grochowski at the plant in the past, but he had not worked there recently, Vidal said. The U.S. Nuclear Regulatory Commission monitored the situation.
Source: http://www.centralohio.com/apps/pbcs.dll/article?AID=/BC/200 60124/NEWS01/601240306/1002&template=BC

3. *January 24, Sun−Sentinel (FL)* — **Florida seeks ways to protect electrical system from hurricanes.** The horrific electrical outages from Hurricane Wilma took center stage Monday, January 23, as state regulators discussed how to harden the power system to withstand more frequent hurricanes. The Florida Public Service Commission made clear that it expected quick decisions on many of the proposals so that the necessary bills can be drafted in time for the spring session of the state Legislature. Among the ideas: Make it easier for cities to put lines underground; change laws to make it easier for power companies to trim trees; install stronger poles; install more poles; and protect substations against flying debris. The workshop is one of several initiatives in Florida to brace the power grid against an onslaught of hurricanes that could last a generation. Speakers from the power industry emphasized that improvement would cost money, and that the state had to decide what sort of system it wanted to pay for. The commission's staff plans to consider proposals at its February 27 meeting, with the commission sending proposals to the Legislature by early March.
Source: http://mobile.sun−sentinel.com/blackberry/index.php?/news/lo cal/southflorida/sfl−cpower24jan24,0,3147228.story?coll=sfla −news−sfla

4. *January 24, The Morning Call (PA)* — **Pennsylvania utility sets new power generation record.** PPL Corp. of Allentown, PA, set a record for power generation for the fourth year in a row. PPL's plants generated 54.8 billion kilowatt−hours of electricity in 2005. That is up two percent from 2004, when the company generated 53.7 billion kilowatt−hours. The company cited careful planning of plant outages as a main factor in the improved performance. PPL controls 12,000 megawatts of generating capacity in seven states: Pennsylvania, Montana, Maine, Connecticut, New York, Arizona, and Illinois. Since 2001, the number of kilowatt−hours PPL generates each year has increased 18 percent. The company has opened additional plants since 2001, including a natural gas plant in Lower Mount Bethel Township. Spokesperson George Lewis said that shorter outages also allow plants to produce more electricity in the year, and operate more efficiently. PPL operates five plants in Pennsylvania. Among those, the Susquehanna nuclear plant near Berwick generated 18.33 billion kilowatt−hours in 2005, up 1.5 percent from last year. The coal−fired plants at Brunner Island, near Harrisburg, generated 10.2 billion kilowatt−hours, down about two percent from last year. That's partially because of a six−week outage for the installation of a new turbine.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5E%5BfmojrpmWUjf%7D38%7Dbfel%5Dv

[Return to top]

## Chemical Industry and Hazardous Materials Sector

5. *January 25, Baytown Sun (TX)* — **Exxon scrubs "greasy" spill from cars, homes in Texas.** Residents of the Archia Court public housing neighborhood near the Exxon Mobil Baytown, TX, Refinery woke up Monday, January 23, to find their homes and cars covered in an oily film. On Tuesday, January 24, they found crews of Exxon Mobil workers and contractors scrubbing the neighborhood clean. Sometime late Sunday night, January 22, or early Monday morning, a storage tank in the refinery spilled a substance called process gas oil (PGO), a mixture heavy lubricant oil and waxy material used by in the refinery's catalytic cracker units to produce light hydrocarbons, said Jeanne Miller, spokesperson for the company's Baytown complex. The reason for the spill is unknown, Miller said. PGO contains benzene, a known carcinogen. Miller said the company sent a team of risk management personnel to talk to neighborhood residents and take samples from standing water in the streets. Those samples revealed no cause for health concerns, according to Miller. Miller said that when the spill occurred, steam accumulated in the tank filled with 200−degree liquid, and the steam filled with PGO droplets escaped through a vent in the tank and was carried by wind over the refinery fence line and North Airhart Street to drift across the neighborhood.
Source: http://web.baytownsun.com/story.lasso?ewcd=cc8ad76a2b3b5021

[Return to top]

## Defense Industrial Base Sector

6. *January 24, Global Security Newswire* — **Annual U.S. missile defense spending could double.** The annual cost of the Bush administration's missile defense plans could more than

double to $19 billion by 2013, and total $247 billion from 2006 through fiscal 2024, according to a U.S. government report. The report, “The Long−Term Implications of Current Defense Plans and Alternatives: Detailed Update for Fiscal Year 2006,” was produced by the Congressional Budget Office and released this month as an update to a September 2004 report. The study projects an average $13 billion per year cost for missile defense through 2024. The administration requested about $8.5 billion for the program last year for the current fiscal 2006, according to the report. The annual cost should climb rapidly to $19 billion by 2013, due to major equipment purchases, before dropping significantly to about $8 billion annually by 2024, it says. All figures are in 2006 dollars. The projections factor the anticipated costs for development, procurement, operation and maintenance of most major Bush administration missile defense initiatives. Administration officials have said they are pursuing a “layered” approach to missile defense, which involves developing multiple technological approaches to striking various ballistic missiles from land, sea, air and possibly space.
Congressional Budget Office report:
http://www.cbo.gov/ftpdocs/70xx/doc7004/01−06−DPRDetailedUpd ate.pdf
Source: http://www.nti.org/d_newswire/issues/2006_1_24.html#E34392C0

7. *January 24, American Forces Press Service* — **DoD taps industry know−how in ongoing counter−IED efforts.** Deputy Defense Secretary Gordon England called on what he called some of the best minds in the country Tuesday, January 24, to help come up with new solutions to the threat improvised explosive devices (IEDs) pose to U.S. troops. Speaking to some 600 leaders from industry, academia, the national laboratories and all branches of the military at a two−day industry conference focused on the IED threat, England challenged participants to find better ways to counter what has become terrorists' weapon of choice in Iraq and, more recently, Afghanistan. IEDs are the leading cause of U.S. combat deaths and injuries in Iraq, the deputy said. The Joint Improvised Explosive Device Defeat Organization and the National Defense Industrial Association co−sponsored the two−day IED conference at the Ronald Reagan Building and International Trade Center in Washington, DC, to exchange information and explore solutions. In addition to briefing industry leaders about current and evolving challenges, defense and military leaders at the forum encouraged participants to help come up with new ways to confront IEDs. But technical solutions alone won't resolve the IED problem, England told the group. Defeating IEDs requires new technology, new tactics, new techniques and new training methods, he said.
Source: http://www.defenselink.mil/news/Jan2006/20060124_4000.html

8. *January 24, European Defense Agency* — **European Defense Agency urged to focus on communications and transport capabilities for rapid response.** European Union (EU) governments Tuesday, January 24, asked the European Defense Agency (EDA) to focus on improving military capabilities in command, control and communications, air−to−air refueling and heavy transport −− all keys to effective, rapid response to developing crises. The EDA Steering Board, meeting at the level of national capabilities planners, agreed that 2006 would be a decisive year to make progress on the agenda laid out by EU Heads of State and Government at their meetings in Hampton Court and Brussels at the end of last year. The EDA will focus on Software Defined Radio, Satellite Communications, and Space and other airborne surveillance capabilities, and look for areas for collaboration with civil applications. The second major capability focus will be strategic lift, the ability to deploy troops and equipment in support of crisis management or disaster relief operations. Looking to the future, the EDA

will investigate longer term possibilities such as a new generation of heavy transport helicopters and the possible development of high−speed ferries to replace slower sea transport. The final capability focus will be air−to−air refueling, where 11 governments have already agreed to work with the EDA.
Source: http://www.eda.eu.int/news/2006−01−24−0.htm

[Return to top]

## Banking and Finance Sector

9. *January 24, WVBR News (NY)* — **CFCU credit union says customers received phishing scam e−mails.** Following a rash of hoax e−mails to Ithaca, NY area e−mail addresses and mailing lists, CFCU Community Credit Union is warning its customers of the "phishing" attempt, an e−mail−based scam intended to fool credit union customers into revealing their online banking passwords or other private information. A message titled "High Alert" on CFCU's online banking service dated this morning warns of the scheme. CFCU senior vice president for operations Eileen Hegedus says the credit union has "notified the FBI, and we've sent out an e−mail to our home banking users to alert them." The scam e−mail, with a subject line "CFCU Community Credit Union Security Measures," seems well targeted to people in the area, with addressees including Cornell University mailing lists, staff, and students, and those using free WVBR.com e−mail addresses. The bogus e−mail includes a phony list of "unsuccessful attempts to login to your account" from Russian IP addresses, then what appears to be a Web link to CFCU's Website at mycfcu.com. Hidden behind the visible Web address is a link to a Website in Singapore that mimics CFCU's current online banking login page, with a welcome message from CFCU president Bob Witty.
Source: http://today.14850.com/0124cfcuscam.html

10. *January 24, National Journal* — **Cyber crime is growing more professional, officials say.** Leading industry and government officials Tuesday, January 24, agreed that cyber criminals are now more professional and primarily focused on stealing money. The change in hacker motivation −− from seeking fame to seeking fortune −− occurred in 2004 and 2005, said Art Wong, vice president for Symantec, at a roundtable discussion on Capitol Hill sponsored by the company. "Hackers are working for financial profit and gain −− not fame," Wong said. Online miscreants are now more interested in releasing worm viruses that hide and gather personal information, than in inflicting big−splash viruses that take down networks. Even more troubling are botnets, which are specially designed networks for hacking. They are propagating quickly in the United States, Europe, and Asia. In some cases, these botnets are rented out to third−party hackers. As hackers get more sophisticated, they also are becoming more professional −− often working Monday through Friday during daytime hours. Much of the information stolen by hackers reaches the streets, as personal information is sold between criminals, said Larry Johnson, a special agent with the Secret Service.
Source: http://www.govexec.com/story_page.cfm?articleid=33230&dcn=to daysnews

[Return to top]

## Transportation and Border Security Sector

11. *January 25, Government Accountability Office* — **GAO−06−318T: Homeland Security: Visitor and Immigration Status Program Operating, but Management Improvements Are Still Needed (Testimony).** The Department of Homeland Security (DHS) has established a program −− the U.S. Visitor and Immigrant Status Indicator Technology (US−VISIT) −− to collect, maintain, and share information, including biometric identifiers, on selected foreign nationals who enter and exit the United States. US−VISIT uses these biometric identifiers (digital finger scans and photographs) to screen persons against watch lists and to verify that a visitor is the person who was issued a visa or other travel document. Visitors are also to confirm their departure by having their visas or passports scanned and undergoing finger scanning at selected air and sea ports of entry. The Government Accountability Office (GAO) was asked to testify on (1) the status of US−VISIT and (2) DHS progress in implementing recommendations that GAO made as part of its prior reviews of US−VISIT annual expenditure plans. The testimony is based on GAO's prior reports as well as ongoing work for the House Committee on Homeland Security. GAO's recommendations are directed at helping the department improve its capabilities to deliver US−VISIT capability and benefit expectations on time and within budget. According to DHS, the recommendations have made US−VISIT a stronger program.
Highlights: http://www.gao.gov/highlights/d06318thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−318T

12. *January 25, Department of Transportation* — **New inspection program to target rail safety hot spots.** A new program to deploy federal railroad inspectors to safety hot spots will begin early this year, Department of Transportation Secretary Norman Y. Mineta announced on Wednesday, January 25, during an update on his Department's National Rail Safety Action Plan. Mineta said the Department expects to start by March a new inspection program that will use accident data to identify rail safety problems for specific railroads and states. The inspection plan will allow federal inspectors to focus their efforts where safety issues are most likely to arise so they can be corrected before a serious train accident occurs, Mineta added. Over the coming months, the Department also will deploy two new track inspection vehicles, tripling the number of miles of track inspected each year; propose a new federal rule to address common human errors that lead to train accidents such as improperly lined switches; and undertake research into train operator fatigue, near misses, and the strength of hazardous materials tank cars, he noted. Mineta unveiled the plan in May 2005, which lays out an aggressive agenda to target the most frequent, highest risk causes of train accidents; better utilize federal rail inspection resources; and accelerate research efforts.
National Rail Safety Action Plan: http://www.dot.gov/affairs/frasafetyplan012506.htm.
Mineta's remarks: http://www.dot.gov/affairs/minetasp012506.htm.
Source: http://www.dot.gov/affairs/dot1006.htm

13. *January 25, Associated Press* — **U.S.−Canada border crossing closed after chase.** A high−speed chase that ended in gunfire closed the U.S.−Canadian border crossing near Blaine, WA, Tuesday, January 24, authorities said. Two men sought in a California homicide were arrested after one of them was shot and wounded. The crossing is one of the busiest on the U.S. northern border. Traffic was diverted to the Pacific Highway crossing about a mile to the east as police investigated. An unspecified number of Canadian border agents, who are unarmed, left their posts during the incident because they were concerned about their safety, said Paula

Shore, a spokesperson for the Canada Border Services Agency. Managers took over and security was not compromised, she said. After a tip that two men sought in the California case could be headed to the area, a car carrying two men matching the description was seen about six miles south of the border on Interstate 5. When a sheriff's deputy tried to stop the car, the occupants sped off, reaching speeds of 100 mph, Sheriff Bill Elfo said. The chase ended just a few feet from the border when a deputy blocked the suspects' car with his squad car, Elfo said. One man bolted, but authorities quickly caught him.
Source: http://www.cnn.com/2006/US/01/25/border.closed.ap/

**14.** *January 25, Star−Ledger (NJ)* — **PATH station to test bomb−detection plan.** A temporary airport−like security system to detect explosives will be set up next month at the Exchange Place PATH (Port Authority Trans−Hudson) station in Jersey City as the first phase of a federal test program designed to increase up rail safety across the country, officials said on Tuesday, January 24. Between February 6 and March 1, the roughly 15,000 passengers who use the station each day will encounter X−ray baggage machines, walk−through metal−detectors and other screening devices. Unlike the security systems at airports, the Rail Security Project will not require passengers to empty their pockets, turn off their laptops or take off their shoes when being screened. If alarms sound, bags may be swiped to check them electronically for explosive residue and passengers may be subjected to a follow−up search with a hand−held wand, officials said. Screeners at Exchange Place will be private contract employees from San Francisco International Airport who will be on loan from the Transportation Security Administration. "We definitely need to look into ways to increase the security of our rail system," said Larry Orluskie, a spokesperson for the Department of Homeland Security.
Source: http://www.nj.com/news/ledger/jersey/index.ssf?/base/news−2/113816869533610.xml&coll=1

**15.** *January 25, Air Cargo News* — **Cargo security summit targets gang theft.** Sponsored by the Florida Statewide Commercial Vehicle Cargo Theft Task Force, the Florida Trucking Association, and the International Cargo Security Council, the 2006 Cargo Security Legislative Summit will be held in Tallahassee, FL, January 25 and 26. It will focuses mainly on truck security, but will also consider several points vital to air cargo. Marion, FL, Sheriff Capt. Tommy Bibb, one of the event organizers, said that each year at least $10 billion of cargo is stolen from warehouses, 18−wheelers, and ship containers. One highlight: the Summit will include an FBI update on the growing threat of Mara Salvatrucha, or MS−13, to officers on the street. The International Cargo Security Council is an association of professionals active in intermodal transportation and supply chain security.
Source: http://www.aircargonews.com/060125/cargosecurity.etihadtraxo n.html

**16.** *January 25, USA TODAY* — **NTSB: Pilots' conduct, fatigue elements of Missouri crash.** A pair of wisecracking pilots on duty for 14 1/2 hours made several grave mistakes just before crashing more than a mile from a runway in Missouri, killing themselves and 11 others, federal investigators said Tuesday, January 24. The National Transportation Safety Board (NTSB) blamed the October 19, 2004, accident on errors by the pilots, who flew too low in darkness and clouds on the way toward Kirksville Regional Airport. The pilots' unprofessional behavior and fatigue likely contributed to the crash, the board ruled. The Jetstream 32 twin−propeller plane struck a line of trees and burst into flames, trapping 13 of the 15 on board. Investigators said they were troubled by the pilots' banter on the flight as the plane got ready to land. Federal

law forbids airline pilots from any joking or casual conversation when the plane dips below 10,000 feet. The crash is the second in two years involving pilots who were joking in the cockpit. Two pilots on an empty Pinnacle Airlines flight died October 14, 2004, after losing control at high altitude. The NTSB called on the Federal Aviation Administration to revise the regulations that allowed the crew to work so long and to require airlines to improve training on fatigue.
Source: http://www.usatoday.com/travel/news/2006−01−24−crashinvestig ation_x.htm

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

17. *January 25, Daily Times (MD)* — **More poultry to be avian flu tested.** The Maryland Department of Agriculture and poultry industry have reached an agreement to immediately conduct testing on the Delmarva Peninsula of all commercial poultry flocks for avian influenza, state officials said Monday, January 23. Daniel Bautista, lab director and poultry diagnostician for the Salisbury Animal Health Diagnostic Laboratory, said the increased testing for the disease −− which is highly contagious among chickens and can wipe out entire flocks −− will be a big undertaking for his small staff. Prior to the new volume testing, Bautista said his staff tested 40 percent of the flocks from more than 2,000 Delmarva farms through the National Poultry Improvement Plan, a federal−state−poultry industry program that monitors avian influenza for commercial flocks. In 2004, a few cases of the illness were found in Worcester, MD, and in Delaware, forcing those farmers to quarantine their land to keep from transmitting the disease. Since then, no incidents have been reported or detected, Bautista said. Tests are conducted every time the farms grow chickens, he said, and the average farm grows five chicken batches a year. Bautista said his lab will test a sample of 11 birds per farm.
Source: http://www.delmarvanow.com/apps/pbcs.dll/article?AID=/200601 25/NEWS01/601250302/1002

18. *January 25, Pratt Tribune (KS)* — **Chronic wasting disease confirmed in Kansas deer herd.** The National Veterinary Services Laboratory in Ames, IA, has verified the preliminary lab test, which was positive for Kansas' first occurrence of chronic wasting disease (CWD) in a wild deer. Tissue samples from the deer, taken by a resident hunter in Cheyenne County during the state's firearms season in December, were initially tested at a Kansas State University lab, then submitted to the lab in Iowa for confirmation. Kansas Department of Wildlife and Parks (KDWP) biologists will sample more deer in Cheyenne County to help determine whether the disease exists in other deer in the vicinity. KDWP also is planning to conduct a public meeting in St. Francis to provide more information on CWD and strategies to minimize the spread of the disease. KDWP biologists have collected tissue samples from deer taken by Kansas hunters since 1996 to monitor deer herd health.
CWD information: http://www.cwd−info.org/

Source: http://www.pratttribune.com/articles/2006/01/24/news/02_deer .txt

19. *January 25, Southeast Farm Press* — **Georgia system prevents diseases and insects from leaving port.** For eight years, University of Georgia (UGA) Cooperative Extension county agents have used digital images, computers and e−mails to quickly diagnose insect and disease problems. Now a UGA team has installed their system in Honduras to protect U.S. farmers and consumers. Called Distance Diagnostics through Digital Imaging (DDDI), the system is in most UGA Extension county offices statewide. UGA shared the technology with 12 other U.S. land−grant universities and then added Honduras as its first international partner. Two DDDI systems have been set up at the Port of Cortez to prevent plant diseases and insects from leaving Honduras. “This is one of only a handful of U.S. Customs offices set up in ports outside the U.S.,” says Marco Fonseca, a UGA Extension horticulturist. “A U.S. inspector checks the shipments, so now agricultural products can go straight into our market.” Fonseca says the U.S. benefits are twofold: The nation is further protected from plant diseases and insects entering its borders, and Americans get fresher imported fruits and vegetables. Inspectors are trained to look for pathogens and pests common to the region. “Barriers like this slow down the movement of pathogens and pests,” he says.
Source: http://southeastfarmpress.com/news/012506−Georgia−pests/

20. *January 24, Associated Press* — **Laurel Park horse has equine herpes.** A horse at Laurel Park, in Maryland, has tested positive for the equine herpes virus that has already claimed two horses at nearby Pimlico Race Course and prompted a state quarantine at the home of the Preakness Stakes. However, the Laurel horse has not shown any symptoms of the disease and it is not clear whether the horse is contagious, or merely has been exposed to the virus in the past like many other horses, said Guy Hohenhaus, state veterinarian for the Maryland Department of Agriculture. The horse, an outrider used in training race horses, has been brought to Pimlico for isolation and further testing. The tests will most likely be in the form of nasal swabs that will be cultured to see if the virus is present in the respiratory tract as well as in the bloodstream. If the swabs test positive, "then that horse probably needs to be restricted until it tests negative," Hohenhaus said. At least 11 horses at Pimlico have shown signs of the virus this month and two horses have been euthanized. Isolation at Pimlico is expected to continue at least until the middle of next month.
Equine Herpes information: http://duke.usask.ca/~misra/virology/stud2004/evd/ehv1page.h tml
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/01 /24/AR2006012400974.html

[Return to top]

## Food Sector

21. *January 25, Associated Press* — **Taiwan lifts ban on U.S. beef imports.** Taiwan said Wednesday, January 25, it was lifting a ban on U.S. beef imports but warned it could reconsider the decision if steps aren't followed to prevent beef at higher risk of being infected with mad cow disease from entering the country. The ban was imposed last June after an American cow was found to be infected with mad cow disease. In a statement, Taiwan's Department of Health said an investigation had shown there was no danger to the country's population, and the import of American beef could resume. Taiwan said, however, that all imported beef will have to carry

a label of approval from the U.S. Department of Agriculture. Only meat from cows aged 30 months or younger will be allowed, while parts like brains, spinal cords, and certain bones will be banned because they carry a higher infection risk, the statement said. The announcement ended Taiwan's second ban on U.S. beef. A previous ban had been in force from late 2004 until April 2005. The U.S. had been the source of 20 percent of Taiwan's beef.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/n/a/2006/01/25/financial/f010510S92.DTL&type=health

22. *January 25, Associated Press* — **Beef industry given a refresher on Japan's requirements.** Japan halted imports of U.S. beef on Friday, January 20, after finding a shipment that contained backbone, which Asian countries consider at risk for mad cow disease. The cuts −− veal hotel rack, which has rib bones connected to the spine −− are eaten in the U.S. but not allowed in Japan. At an Agriculture Department meeting hastily arranged by Agriculture Secretary Mike Johanns, a National Meat Association official called the error "a setback and a great embarrassment" to other companies in the industry. The error jeopardized a market worth $1.4 billion in 2003, the year before Japan banned the importation of American beef. Only weeks ago Japan reopened its market, which had been closed since the U.S. discovered its first case of mad cow disease in December 2003. About three dozen companies and industry groups were represented at the meeting in an U.S. Department of Agriculture auditorium. Johanns summoned them for a refresher course on export rules and filling out forms.
Source: http://www.dfw.com/mld/dfw/news/breaking_news/13707665.htm

23. *January 24, Columbus Dispatch (OH)* — **Guide gives grocers assist on food safety.** Grocers have new guidelines to help them keep their food safe from terrorists. The Retail Food Defense Preparedness Guide, available as a CD−ROM, gives grocers detailed information to help them assess and address any vulnerability in their food supply −− from the delivery of the products to the retail stores to the time it leaves the store with the customer. The guide was put together by the Ohio departments of agriculture, health and public safety. The free guide is being distributed to 16,000 retailers statewide, said Tom Jackson, president of the Ohio Grocers' Association, which created the guide with the Ohio Department of Agriculture. New York and New Jersey have created similar food security tips, based on rules and regulations from the Bioterrorism Act of 2002, said Brenda Zimmer of the U.S. Food and Drug Administration's Cincinnati, OH, office.
Ohio Department of Agriculture statement:
http://www.ohioagriculture.gov/news/news/2006/food−012306−fo oddefense.pdf
Source: http://www.columbusdispatch.com/business−story.php?story=dispatch/2006/01/24/20060124−C1−04.html

[Return to top]

## Water Sector

24. *January 25, Chicago Tribune (IL)* — **Radioactive leak taints water.** A plume of radioactive tritium seeping into groundwater near a Will, IL, nuclear power plant has prompted Exelon Corp. to buy out one nearby property owner and offer to compensate 14 others for any loss in home value. Levels of the radioactive isotope found outside the Braidwood Generating Station so far have been well below the amount the federal government considers unhealthy. But the

company acknowledged Tuesday, January 24, that there is more tritium in the nearby groundwater than occurs naturally and vowed to clean it up. In one well on Exelon's property, the amount of tritium was more than 11 times higher than the federal limit for groundwater, according to the Nuclear Regulatory Commission. Based on that finding and tests of 15 nearby private wells, the Illinois Environmental Protection Agency cited Exelon, the parent company of ComEd, for two violations of the state's groundwater standards and gave company officials until February 3 to file a report detailing what they know about the tritium plume. Exelon has traced the tritium to a 1998 pipeline leak that wasn't thought at the time to contain significant amounts of radioactive material. The pipe pumps water from the plant's cooling lake to the Kankakee River five miles away.
Source: http://www.chicagotribune.com/news/nationworld/chi−0601250209jan25,1,1527963.story?track=rss

[Return to top]

## Public Health Sector

**25.** *January 25, Associated Press* — **China bird flu death toll hits seven.** A woman in southwestern China has died from bird flu, bringing the country's human death toll from the disease to seven, the official Xinhua News Agency said Wednesday, January 25. The news agency reported Monday, January 23, that the woman showed symptoms for a fever and pneumonia on January 12 and was hospitalized in a critical condition in Chengdu in Sichuan province. She tested positive for the H5N1 strain of bird flu on January 17.
Source: http://edition.cnn.com/2006/WORLD/asiapcf/01/25/china.bird.f lu.ap/

**26.** *January 25, Associated Press* — **Drug makers plan big increase in flu vaccine for next fall.** Pharmaceutical companies say they are preparing to produce as many as 120 million doses of flu vaccine for the next flu season, by far the most ever. The increased production could mean an end to the shortages of the past several years, especially in the 2004−5 flu season, when bacterial contamination led to the shutdown of a British factory that was to produce nearly half the United States' supply. Speaking Tuesday, January 24, at a flu vaccine conference sponsored by the American Medical Association and the U.S. Centers for Disease Control and Prevention, vaccine makers said the increase was warranted for several reasons: better government reimbursement for shots, indications that federal health officials may one day recommend flu shots for nearly everyone, and public fears of avian flu (although the vaccine would protect only against conventional flu). GlaxoSmithKline, which produced 7.5 million doses of flu vaccine for the current flu season, said it expected to distribute 20 million to 30 million for next season. Sanofi Pasteur, the main vaccine producer for the current season, broke ground last July on a vaccine plant in Swiftwater, PA, to double the capacity of that company.
Source: http://www.nytimes.com/2006/01/25/national/25flu.html?_r=1

**27.** *January 25, Boston Globe (MA)* — **Flu vaccine distribution flawed.** The nation's top disease tracker Tuesday, January 24, acknowledged that there are significant flaws in the flu vaccine−distribution system in the U.S. and pledged to consider expanding the federal government's role in buying and tracking shots. For the current flu season, the U.S. Centers for Disease Control and Prevention (CDC) bought about 11.5 million doses −− out of 86 million produced by private manufacturers −− with much of it then resold to state health departments.

"Since we don't own the supply, it's very difficult for us to put our weight behind supporting appropriate distribution," said Julie Gerberding, CDC director, speaking at a summit on the flu vaccine supply and its distribution. Doctors and public health authorities voiced concern about the patchwork system of public agencies and private doctors, pharmacies, and big−box retailers that now provide flu vaccine. Health authorities said they are particularly dismayed by the failure to establish a network that would follow every shot from the time it left a manufacturer to the time it was administered. A detailed tracking system, public health officials said, has the potential to ease a persistent supply−demand mismatch that results most years in millions of vaccine doses being squandered. The CDC is studying such a tracking system.
Source: http://www.boston.com/news/nation/articles/2006/01/25/flu_vaccine_distribution_flawed_cdc_contends/

**28.** *January 25, Agence France−Presse* — **Indonesia reports another bird flu case as WHO warns over markets.** A 22−year−old chicken seller is Indonesia's latest bird flu case, an official said, as the World Health Organization (WHO) warned that traditional markets must clean up their act to curb the spread of the virus. Local tests showed the Jakarta man tested positive for the virus. He was admitted to the main hospital treating bird flu patients Thursday, January 19, health ministry official Hariyadi Wibisono said Wednesday, January 24. Fourteen people have died of the H5N1 strain of avian influenza in Indonesia, the world's fourth most populous country where many people live in close contact with poultry, even in urban areas. Six other human cases in Indonesia have been confirmed but the patients survived. Three others suspected of carrying the virus are being treated. Meanwhile, officials from the World Health Organization (WHO) who toured an animal market in the capital said improving waste management and sanitation systems was the top challenge facing traditional wet markets here. "Where do you reduce the exposure of people to the disease, how do you improve the hygiene and the safety of the food supply and ways to improve waste management. These are the key challenges," Peter Karim Ben Embarek, a scientist with the WHO's food safety department said.
Source: http://news.yahoo.com/s/afp/20060125/hl_afp/healthfluindonesia_060125124209;_ylt=AkdJ7r_Yln0w_4F.CFunU66JOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

**29.** *January 25, Reuters* — **Scientists follow the money to predict epidemics.** Researchers in Germany and the U.S. tracked the circulation of dollar bills to develop a mathematical model of human travel that can be used to plot the spread of future pandemics. "There are some universal rules governing human travel and they can be used to develop a new class of model for the spread of infectious disease," said Dirk Brockmann, of the Max Planck Institute in Goettingen, Germany. "We can now plug in the parameter ranges that we think will apply to influenza and then simulate a pandemic that runs through Europe and see what happens." Mathematical models and computer simulations could also help to develop measures to take against it, he added. Human movement is a main cause of the spread of infectious disease but with modern−day travel involving boats, planes, trains, cars and other means of transport it is virtually impossible to compile a comprehensive set of data on travel. The scientists analyzed information from an online bill−tracking Internet site. The information from the site enabled the researchers to develop a mathematical theory of human travel behavior. When they compared their results with traffic flow of aviation networks in the U.S., they found it correlated closely.
Source: http://www.thanhniennews.com/worlds/?catid=9&newsid=12273

30. *January 25, Star−Ledger (NJ)* — **Hospitals receive funds for emergency preparedness.** The New Jersey Health Department Tuesday, January 24, awarded five million dollars in grants to New Jersey hospitals and other health care facilities in an effort to strengthen emergency response. Eighty acute−care hospitals and 14 federally qualified health centers will use the money to enhance their ability to respond to chemical, biological, radiological, nuclear, and explosive incidents. The grants were made available through funding from the Federal Health Resource and Services Administration. Facilities can use the money to purchase equipment to expand isolation, decontamination, and communication capabilities and to increase pharmaceutical supplies and personal protection equipment. The grant also can be used for staff education and training to conduct preparedness drills and exercises.
Source: http://www.nj.com/news/ledger/jersey/index.ssf?/base/news−2/113816852633610.xml&coll=1

[Return to top]

## Government Sector

Nothing to report.
[Return to top]

## Emergency Services Sector

31. *January 25, Government Accountability Office* — **GAO−06−335T: Federal Emergency Management Agency: Challenges for the National Flood Insurance Program (Testimony).** The National Flood Insurance Program (NFIP), established in 1968, provides property owners with some insurance coverage for flood damage. The Federal Emergency Management Agency (FEMA) within the Department of Homeland Security is responsible for managing the NFIP. The unprecedented magnitude and severity of the flood losses from hurricanes in 2005 challenged the NFIP to process a record number of claims. These storms also illustrated the extent to which the federal government has exposure for claims coverage in catastrophic loss years. FEMA estimates that Hurricanes Katrina, Rita, and Wilma will generate claims and payments of about $23 billion −− far surpassing the total claims paid in the entire history of the NFIP. This testimony provides information from past and ongoing Government Accountability Office (GAO) work on issues including: (1) NFIP's financial structure; (2) the impact of properties with repetitive flood losses on NFIP's resources; (3) proposals to increase the number of policies in force; and (4) the status of past GAO recommendations. In past work, GAO recommended that FEMA strengthen its oversight of the NFIP and develop plans to implement requirements of the Flood Insurance Reform Act of 2004. FEMA disagreed with those recommendations.
Highlights: http://www.gao.gov/highlights/d06335thigh.pdf
Source: http://www.gao.gov/new.items/d06335t.pdf

32. *January 25, U.S. Department of Energy* — **Department of Energy supercomputers to analyze hurricane coastal surges, help plan rebuilding in Louisiana, Gulf Coast.** The U.S. Department of Energy's Office of Science has allocated 400,000 processor hours of supercomputing time at its National Energy Research Scientific Computing (NERSC) Center to

the U.S. Army Corps of Engineers New Orleans District to run a series of simulations of hurricane protection projects within coastal Louisiana. The Army Corps of Engineers has been asked by the Federal Emergency Management Agency (FEMA) to run a series of simulations estimating hurricane−induced storm surge elevations as part of FEMA's Map Modernization Program to update Flood Insurance Rate Maps in other areas. The data collected from the simulations will provide valuable flood elevation data that will be used by FEMA to develop new flood hazard information. Additionally, FEMA has asked the Corps' New Orleans District to speed up development of new flood insurance studies in areas where they are working on them. Because of coastal inundation induced by Hurricanes Katrina and Rita, the New Orleans District has begun to rebuild and enhance the existing flood control system, as well as design a new system. This design will offer a higher level of protection to the city of New Orleans and coastal Louisiana while at the same time encompassing the state's coastal ecosystem.
NERSC Center Website: http://www.nersc.gov/
U.S. Army Corps of Engineers Website: http://www.usace.army.mil/
Source: http://www.energy.gov/news/3103.htm

**33.** *January 24, Federal Computer Week* — **West Virginia miners to get electronic tracking devices.** West Virginia lawmakers unanimously passed legislation Monday, January 21, requiring miners to wear electronic tracking devices and carry wireless emergency communications equipment when working underground. Swift passage of the bill was in direct response to the deaths of 14 miners in two separate incidents since the beginning of this year. Governor Joe Manchin is expected to sign the bill into law. Under the legislation, miners, who will receive training on the communications equipment and refresher courses each year, should be able to receive communications at any location throughout the mine from the surface. During accidents or other emergencies, tracking devices would provide real−time monitoring and physical location of miners underground. The bill also makes it a crime to tamper with or knowingly remove communications equipment or tracking devices. The legislation also creates a rapid response system that includes an around−the−clock emergency operations center and an updated list of contact information. The National Mining Association also announced the formation of a Mine Safety Technology and Training Commission that will examine safety procedures and training communications technologies, mine rescue technology, and necessary policy changes. The commission will make preliminary recommendations in July and issue final ones by the end of the year.
Source: http://fcw.com/article92067−01−24−06−Web

**34.** *January 24, Government Technology* — **Kentucky governor presents check for first responders' equipment.** Governor Ernie Fletcher on Tuesday, January 24, presented a $126,934 homeland security check to Washington County to fund communications equipment for the county's first responders. "Ensuring that our commonwealth's first responders can communicate effectively is a critical concern that we are addressing throughout Kentucky," said Governor Fletcher. The homeland security check presented Tuesday will provide the county with repeaters that will fix communications "dead spots" and allow first responders, many of whom may have different types of radio equipment, the ability to talk to one another via that equipment. The governor also named the City of Springfield and Washington County as "Prepared Kentucky Communities;" the result of a five−day vulnerability assessment conducted by security professionals with the Kentucky Community Preparedness Program. Assessors analyzed facilities, structures and security policies and their relationship to each other in order

to identify the community's weaknesses and analyze preparedness levels. The team then presented a report of recommendations for improvements. Local officials formed a group to discuss areas of concern raised by the assessment and they have worked to ensure each of the sites assessed received and understood the recommendations made by the assessment team.
Source: http://www.govtech.net/magazine/channel_story.php/98013

[Return to top]

## Information Technology and Telecommunications Sector

**35.** *January 25, USA TODAY* — **Free Website to list programs with spyware.** A free Website, StopBadware.org, launched Wednesday, January 25, plans to provide a list of programs that contain spyware and other malicious software. It will also identify companies that develop the programs and distribute them on the Internet. Consumers can then decide if a program is safe to download. "For too long, these companies have been able to hide in the shadows of the Internet," says John Palfrey, who heads the Berkman Center of Internet & Society at Harvard Law School and is spearheading the project. "What we're after is a more accountable Internet." The initiative is being run by Harvard and the Oxford Institute and is backed by high−tech heavyweights including Google and Sun Microsystems. Consumer Reports' WebWatch is serving as a special adviser. In addition to spyware, the hit list of the StopBadware coalition includes malicious "adware" programs that serve up onslaughts of pop−up ads or software that contains hidden viruses and worms. By checking StopBadware.org, its organizers say, consumers can choose, in the first place, not to download a program containing the malicious software. The coalition is encouraging consumers to visit the Website to log their experiences with harmful programs.
StopBadwar.org Website: http://www.stopbadware.org/
Source: http://www.usatoday.com/tech/news/computersecurity/2006−01−2 5−spyware_x.htm

**36.** *January 25, Shelbyville Times−Gazette (TN)* — **Cell towers in Tennessee hit by gunshots.** Thousands of dollars worth of gunshot damage was done to electronic equipment and beacons at communications towers near the crest of Horse Mountain north of Shelbyville, TN, early Monday afternoon, January 23. "Bedford County Board of Education's wireless Internet and T−1 service was lost and antennas for the Bedford County Sheriff's Department (BCSD), Volunteer Fire Services Inc. and Shelbyville Fire Department are on the towers," John Hettish, president of Middle Tennessee Two−Way Inc., said. Ten antennas are located on two towers atop the mountain, Hettish said. They include cellular phone services for several firms as well as law enforcement radio antennas. Monday's damage occurred about 1 p.m. CST, Hettish said, and included an estimated $28,000 worth of damage to Trillion Data Communications equipment inside a ground−level cabinet near the towers' base. Several bullets went completely through the cabinets, according to a photo provided by Hettish. An estimated $4,000 damage was done to equipment owned by The Cromwell Group of Nashville, owner of one of the towers, Hettish said. A global positioning system antenna atop a Verizon Wireless substation was shot and destroyed between 2:45−3:15 p.m. CST, Sgt. Billy Prince of the BCSD said.
Source: http://www.t−g.com/story/1136969.html

**37.** *January 24, Tech Web* — **Kama Sutra worm spoofs digital certificates.** The Kama Sutra worm can fool Windows into accepting a malicious ActiveX control by spoofing a digital

signature, a security company said Tuesday, January 24. Sunnyvale, CA−based Fortinet said the worm −− which also goes by names such as Nyxem.e, MyWife.d, Grew.a, and Blackmal.e −− adds 18 entries to the Windows Registry to slip the ActiveX control by the operating system's defenses. "By creating the following entries, the control is considered 'safe' and digitally signed," said the Fortinet advisory. The ActiveX control, added Fortinet, is used by the worm to automatically run its code each time the PC is turned on and Windows boots. "The threat of worms like this will make them much more dangerous in the future," said Bojan Zdrnja, an analyst for the Internet Storm Center, on the group's site. As of late Monday, January 23, the Kama Sutra worm had infected more than 630,000 systems, said the Internet Storm Center. The worm is considered particularly dangerous because it contains code that triggers an overwrite of all .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp files on the third of each month.
Source: http://www.securitypipeline.com/news/177103403;jsessionid=BWMKMS524JJFQQSNDBGCKHSCJUMEKJVN

**38.** *January 24, Register (United Kingdom)* — **Seventy−seven percent of Google users don't know it records personal data.** More than three quarters of Web surfers don't realize Google records and stores information that may identify them, results of a new opinion poll show. The phone poll, which sampled over 1000 Internet users, was conducted by the Ponemon Institute. Google maintains a lifetime cookie that expires in 2038, and records the user's IP address. But more recently it has begun to integrate services which record the user's personal search history, e−mail, shopping habits, and social contacts. After first promising not to tie its e−mail service to its search service, Google went ahead and opted its users in anyway. It's all part of CEO Eric Schmidt's promise to create a "Google that knows more about you."
Source: http://www.theregister.co.uk/2006/01/24/google_privacy_poll/

**39.** *January 24, Tech Web* — **Bill Gates' spam prediction misses target.** On January 24, 2004, Bill Gates told a group at the World Economic Forum that "two years from now, spam will be solved." During the talk, Gates pinned his prediction on the creation of an authentication scheme to verify senders' identities, as well as the hope that some kind of micropayment structure could be created for levying fees on e−mail. "We have a long way to go before we solve the spam problem," said Scott Chasin, the chief technology officer for Denver, CO−based e−mail security firm MXlogic. Neither of the proposals Gates mentioned two years ago have made much headway. Although Microsoft uses its own Sender ID authentication protocol for the company's Web−based Hotmail service, neither Sender ID nor the competing DomainKeys from Yahoo have anything like broad acceptance by ISPs or enterprises. And the micropayment concept for e−mail is as dead now as it was two years ago. Microsoft may take the position that "solving" the spam problem means containing spam with filtering technology, Chasin said, but even using that definition, spam remains a huge problem.
Source: http://www.techweb.com/wire/security/177103408;jsessionid=F33FC31KIRIQQSNDBGCKH0CJUMEKJVN

**40.** *January 24, Washington Technology* — **DHS vows to protect info on national database.** The Department of Homeland Security (DHS) has stepped up assurances that it will maintain the confidentiality of critical infrastructure information submitted to the National Asset Database, according to the newly revised draft National Infrastructure Protection Plan (NIPP) Base Plan version 2.0. DHS will evaluate all requests to view the database and will grant access only to

select DHS employees and others on a “tightly controlled, need−to−know” basis, the revised plan states. The new language is set forth in the 234−page NIPP distributed by DHS this week. The plan was delivered by e−mail via NIPP@dhs.gov. The plan establishes a work and time frame for assessing vulnerabilities and risks and coordinating protections for 17 critical infrastructure sectors, including IT and telecommunications. Cybersecurity is treated as a cross−sector responsibility. DHS’ assurances about database access appear to address concerns raised by IT executives and others over protecting confidentiality of the information they might submit on specific vulnerabilities within their sectors. One fear raised by IT industry members is that disclosing weak spots in their own networks may result in leaks that can be exploited by competitors.
Source: http://www.washingtontechnology.com/news/1_1/homeland/27812−1.html

## Internet Alert Dashboard

### DHS/US−CERT Watch Synopsis

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

**US−CERT Operations Center Synopsis:** US−CERT is aware of a new mass mailing worm known as Nyxem (CME−24). This worm relies on social engineering to propagate. Specifically, the user must click on a link or open an attached file.

The Nyxem worm targets Windows systems that hide file extensions for known file types (this is the default setting for Windows XP and possibly other versions). The worm's icon makes it appear to be a WinZip file. As a result, the user may unknowingly execute the worm. For more information please review: http://cme.mitre.org/data/list.html#24

Once a Windows system is infected, the malicious code may:

Attempt to harvest email addresses stored on the infected system

Utilize its own SMTP engine to send itself to the harvested email addresses

Disable anti−virus and file sharing programs

Spread itself using all available Windows network shares on the infected system

Modify the active Desktop

In addition, on February 3, 2006, the worm will destroy files with the following extensions: DOC, XLS, MDB, MDE, PPT, PPS, ZIP, RAR, PDF, PSD and DM.

There is limited information concerning this potential threat, US−CERT strongly encourages users and system administrators to implement the following

workarounds:

Install anti−virus software, and keep its virus signature files up−to−date

Block executable and unknown file types at the email gateway

US−CERT strongly encourages users not to follow unknown links, even if sent by a known and trusted source. Users may also wish to visit the US−CERT Computer Virus Resources for general virus protection information at URL: http://www.us−cert.gov/other_sources/viruses.html

Exploit for Vulnerability in VERITAS NetBackup Volume Manager Daemon
US−CERT is aware of a public exploit for a vulnerability in VERITAS NetBackup Volume Manager Daemon (vmd). The VERITAS NetBackup vmd listens on network port 13701/tcp. An attacker could send a specially crafted packet to the Volume Manager on a vulnerable system to cause a buffer overflow or a denial of service condition. For more information about this vulnerability can be found in the following URL:

VU#574662 VERITAS NetBackup library buffer overflow vulnerability: http://www.kb.cert.org/vuls/id/574662

US−CERT strongly encourages users review the Symantec Advisory SYM05−024 and apply the recommended updates to address this vulnerability:

http://seer.support.veritas.com/docs/279553.htm

http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

**Current Port Attacks**

| | |
|---|---|
| **Top 10 Target Ports** | 1026 (win−rpc), 6881 (bittorrent), 25 (smtp), 445 (microsoft−ds), 80 (www), 32768 (HackersParadise), 139 (netbios−ssn), 135 (epmap), 2234 (directplay), 113 (auth)<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

**41.** *January 25, Wall Street Journal* — **To protect New York, police study London's effort.** As New York law enforcement agencies and businesses consider how to improve security as part of the plan to rebuild lower Manhattan, they are looking to London for ideas on guarding against potential terrorist attacks and fighting crime. The hallmark of London's strategy is what officials call "the ring of steel," which refers to closed−circuit cameras and narrow roads that

encircle the City of London. "In creating the plan for the World Trade Center site, we are looking at best practices around the globe as we seek to create a new state−of−the−art security model," said James Kallstrom, counterterrorism adviser to New York Governor George Pataki and designer of the new World Trade Center site's security plans. Similarities between lower Manhattan and the City of London are likely to help authorities with their planning. Both neighborhoods are about a square mile in area. Some 300,000 commuters travel through each area daily. Both are global financial hubs, with banks and stock exchanges that remain targets for terror attacks. And, in both cities, the subways are major funnels bringing people into the neighborhoods and vulnerability points.
Source: http://www.post−gazette.com/pg/06025/644077.stm

[Return to top]

## General Sector

**42.** *January 25, Associated Press* — **Arkansas chemical weapons site tightens security.** The Army stepped up security at an arsenal where chemical weapons are stored after three people entered a restricted zone, officials said Wednesday, January 25. The security measures were taken as a precaution at the Pine Bluff Arsenal after the intrusion at a forested federal preserve 30 miles south of Little Rock. Officials didn't know what the three people were doing there, spokesperson Cheryl Avery said. "We are still assessing the situation," Avery said. The Arkansas Department of Emergency Management was notified of the intrusion but was given no indication of the seriousness of the incident, said spokesperson Kathy Hedrick. The Pine Bluff Arsenal stores 12 percent of the military's chemical weapons, which include nerve gas and mustard gas. It is the nation's second largest stockpile. The materials are being incinerated, and officials have said that will take about five years to complete.
Source: http://www.cnn.com/2006/US/01/25/arsenal.security.ap/index.h tml

[Return to top]

**DHS Daily Open Source Infrastructure Report Contact Information**

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

**DHS Daily Open Source Infrastructure Report Contact Information**

| | |
|---|---|
| Content and Suggestions: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644. |
| Subscription and Distribution Information: | Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information. |

## Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

## Department of Homeland Security Disclaimer

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